Guida per l'utente

AWS CloudTrail

Version 1.0

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

AWS CloudTrail: Guida per l'utente

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

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

Table of Contents

Che cos'è AWS CloudTrail? ... 1
Accedendo CloudTrail ... 2
CloudTrail console ... 3
AWS CLI ... 3
CloudTrail APIs ... 4
AWS SDKs ... 4
Come CloudTrail funziona ... 4
CloudTrail Cronologia degli eventi ... 5
CloudTrail Archivi di dati dei laghi e degli eventi ... 5
CloudTrail Cruscotti di Lake ... 8
CloudTrail sentieri ... 9
CloudTrail Eventi Insights ... 14
CloudTrail canali ... 16
Concetti ... 16
CloudTrail eventi ... 17
Cronologia degli eventi ... 43
Trail ... 43
Percorsi organizzativi ... 46
CloudTrail Archivi di dati su laghi ed eventi ... 47
CloudTrail Approfondimenti ... 48
Tag ... 48
AWS Security Token Service e CloudTrail ... 49
Eventi dei servizi globali ... 49
Regioni supportate ... 51
Servizi e integrazioni supportati ... 55
AWS integrazioni di servizi con registri CloudTrail ... 56
CloudTrail integrazione con Amazon EventBridge ... 58
CloudTrail integrazione con AWS Organizations ... 59
CloudTrail integrazione con AWS Control Tower ... 59
CloudTrail integrazione con Amazon Security Lake ... 60
CloudTrail Integrazione di Lake con Amazon Athena ... 60
CloudTrail Integrazione di Lake con AWS Config ... 60
CloudTrail Integrazione lacustre con AWS Audit Manager ... 60
AWS argomenti di servizio per CloudTrail ... 60

Servizi non supportati ... 88
Quote in AWS CloudTrail ... 89
CloudTrail quote di risorse ... 89
Quote di transazioni al secondo (TPS) in CloudTrail ... 95
CloudTrail tutorial ... 96
Concedi le autorizzazioni di utilizzo CloudTrail ... 96
Visualizza la cronologia degli eventi ... 98
Crea un percorso per registrare gli eventi di gestione ... 99
Visualizzare i file di log ... 102
Crea un archivio dati di eventi per gli eventi di dati S3 ... 103
Visualizzazione CloudTrail dei costi e dell'utilizzo ... 109
Utilizzo Budget AWS per gestire i costi ... 114
Creazione di tag di allocazione dei costi definiti dall'utente per i data store di CloudTrail eventi Lake ... 114
Gestione dei costi dei CloudTrail percorsi ... 115
Configurazione dei percorsi ... 115
Consulta anche ... 117
Gestione dei costi CloudTrail del lago ... 117
Opzioni di prezzo del datastore di eventi ... 117
Comprensione delle tariffe CloudTrail del lago ... 119
Consigli su come ridurre i costi ... 121
Consulta anche ... 122
Lavorare con la cronologia CloudTrail degli eventi ... 124
Limitazioni della cronologia degli eventi ... 125
Visualizzazione degli eventi di gestione recenti con la console ... 126
Navigazione tra le pagine ... 127
Personalizzazione dello schermo ... 127
Filtraggio degli eventi CloudTrail ... 129
Visualizzazione dei dettagli per un evento ... 131
Download di eventi ... 131
Visualizzazione di risorse a cui viene fatto riferimento tramite AWS Config ... 132
Visualizzazione degli eventi di gestione recenti con AWS CLI ... 133
Prerequisiti ... 135
Visualizzazione delle informazioni di aiuto della riga di comando ... 135
Ricerca di eventi ... 136
Specifica del numero di eventi da restituire ... 137

Ricerca di eventi in base a un intervallo di tempo ... 137
Ricerca di eventi in base a un attributo ... 138
Specifica della pagina di risultati successiva ... 139
Recupero dell'input JSON da un file ... 140
Campi di output della ricerca ... 141
Lavorare con CloudTrail Insights ... 144
Costi per gli eventi Insights ... 145
Erogazione di eventi Insights ... 147
Registrazione degli eventi di Insights con la console CloudTrail ... 148
Abilitare CloudTrail Insights su un percorso esistente con la console ... 149
Abilitazione di CloudTrail Insights su un data store di eventi esistente con la console ... 149
Registrazione degli eventi di Insights con AWS CLI ... 150
Registrazione degli eventi di Insights per un percorso utilizzando il AWS CLI ... 151
Registrazione degli eventi di Insights per un archivio dati di eventi utilizzando il AWS CLI ... 152
Visualizzazione di eventi Insights per i percorsi ... 156
Visualizzazione degli eventi Insights per i percorsi con la console ... 157
Visualizzazione degli eventi Insights per i sentieri con AWS CLI ... 164
Visualizzazione degli eventi Insights per i datastore di eventi ... 174
Visualizzazione del dashboard di Insights per un data store di eventi ... 174
Visualizzazione di query di esempio per gli eventi Insights ... 176
Lavorare con CloudTrail Lake ... 177
CloudTrail Archivi di dati sugli eventi Lake ... 177
CloudTrail Domande sul lago ... 178
CloudTrail Dashboard Lake ... 179
CloudTrail Integrazioni Lake ... 180
Risorse aggiuntive ... 180
CloudTrail Regioni supportate dai laghi ... 181
CloudTrail Concetti e terminologia dei laghi ... 183
Datastore di eventi ... 183
Integrazioni ... 185
Query ... 186
Pannelli di controllo ... 186
Datastore di eventi ... 187
Crea, aggiorna e gestisci gli archivi dati degli eventi con la console ... 189
Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI ... 245
Gestione dei cicli di vita dell'archivio di dati degli eventi ... 279

Copia di eventi traccia in un archivio dati degli eventi 280
Federare un datastore di eventi 299
Datastore di eventi dell'organizzazione 311
Integrazioni 319
Crea un'integrazione con un CloudTrail partner tramite la console 320
Crea un'integrazione personalizzata con la console 323
Crea, aggiorna e gestisci le integrazioni di CloudTrail Lake con AWS CLI 327
Ulteriori informazioni sui partner di integrazione 336
CloudTrail Schema degli eventi di Lake Integrations 338
Pannelli di controllo 346
Prerequisiti 348
Limitazioni 348
Supporto delle Regioni 348
Autorizzazioni richieste 349
Visualizza una dashboard gestita 353
Abilita la dashboard Highlights 370
Disattiva la dashboard Highlights 372
Crea una dashboard personalizzata 372
Imposta una pianificazione di aggiornamento per una dashboard personalizzata 376
Disattiva la pianificazione dell'aggiornamento per un pannello di controllo personalizzato 376
Modificare la protezione della terminazione 377
Eliminare una dashboard personalizzata 378
Crea, aggiorna e gestisci i dashboard con AWS CLI 378
Query 178
Strumenti dell'editor di query 397
Crea query su CloudTrail Lake da istruzioni in linguaggio naturale 397
Visualizza interrogazioni di esempio 405
Creazione o modifica di una query 406
Eseguire una query e salvare i risultati della query 407
Visualizzazione dei risultati della query 411
Riassumi i risultati delle interrogazioni in linguaggio naturale 413
Scaricare i risultati della query salvati 414
Convalida dei risultati della query salvati 417
Ottimizza le query 431
Esegui e gestisci le query di CloudTrail Lake con AWS CLI 435
CloudTrail Vincoli Lake SQL 440

Funzioni, condizioni e operatori join supportati ... 441
Supporto avanzato per query multi-tabella ... 442
Schemi SQL supportati per datastore di eventi ... 443
Schema supportato per i campi di registrazione CloudTrail degli eventi ... 444
Schema supportato per i campi di registrazione degli eventi di CloudTrail Insights ... 447
Schema supportato per i campi dei record degli elementi di configurazione AWS Config ... 450
Schema supportato per i campi di registrazione delle prove AWS Audit Manager ... 451
Schema supportato per i campi non associati agli eventi AWS ... 452
CloudWatch Metriche supportate ... 454
Lavorare con i CloudTrail sentieri ... 457
Creare un percorso per il tuo Account AWS ... 458
Creazione e aggiornamento di un percorso con la console ... 459
Creazione, aggiornamento e gestione di percorsi con AWS CLI ... 490
Creazione di percorsi multipli ... 523
Creazione di un percorso per un'organizzazione ... 524
Passaggio dai percorsi degli account dei membri ai percorsi organizzativi ... 528
Preparazione per la creazione di un percorso per la tua organizzazione ... 529
Creazione di un percorso per la tua organizzazione nella console ... 533
Creare un percorso per un'organizzazione con AWS CLI ... 544
Risoluzione dei problemi ... 551
Comprendere i percorsi multiregionali e le regioni opt-in ... 554
Quali sono i vantaggi dei percorsi multiregionali? ... 555
Cosa succede quando si crea un percorso multiregionale? ... 555
Cosa succede quando abiliti una regione opt-in? ... 555
Cosa succede quando si disabilita una regione con consenso esplicito? ... 556
Copiare gli eventi del percorso su CloudTrail Lake ... 556
Considerazioni sulla copia di eventi di percorso ... 558
Autorizzazioni necessarie per la copia di eventi traccia ... 559
Copia gli eventi del trail in un data store di eventi esistente utilizzando la console CloudTrail ... 564
Acquisizione e visualizzazione dei file di CloudTrail registro ... 567
Trovare i file di registro CloudTrail ... 567
Scaricamento dei file di CloudTrail registro ... 569
Configurazione delle notifiche Amazon SNS per CloudTrail ... 570
Configurazione CloudTrail per l'invio di notifiche ... 571
Utilizzo AWS CloudTrail con gli endpoint VPC dell'interfaccia ... 573

Regioni ... 574
Crea un endpoint VPC per CloudTrail ... 574
Crea una policy per gli endpoint VPC per CloudTrail ... 574
Sottoreti condivise ... 578
Requisiti di denominazione ... 578
CloudTrail requisiti di denominazione delle risorse ... 578
Requisiti di denominazione dei bucket Amazon S3 ... 579
AWS KMS requisiti di denominazione degli alias ... 580
Account AWS chiusura e percorsi ... 580
Configurare CloudTrail le impostazioni ... 582
Amministratori delegati dell'organizzazione ... 582
Autorizzazioni necessarie per assegnare un amministratore delegato ... 587
Aggiunta di un CloudTrail amministratore delegato ... 588
Rimozione di un CloudTrail amministratore delegato ... 589
Canali collegati al servizio ... 590
Visualizzazione di canali collegati ai servizi tramite la console ... 590
Visualizzazione dei canali collegati ai servizi utilizzando il AWS CLI ... 591
Comprendere CloudTrail gli eventi ... 594
Eventi di gestione ... 595
Eventi di dati ... 597
Eventi di dati supportati da AWS CloudTrail ... 598
Eventi di attività di rete ... 622
Eventi Insights ... 625
Eventi di gestione ... 628
Eventi di gestione ... 629
Lettura e scrittura di eventi ... 630
Registrazione degli eventi di gestione con AWS Management Console ... 631
Registrazione degli eventi di gestione con la AWS CLI ... 635
Registrazione degli eventi di gestione con la AWS SDKs ... 650
Eventi di dati ... 650
Eventi di dati ... 652
Eventi di sola lettura e di sola scrittura ... 678
Registrazione degli eventi relativi ai dati con il AWS Management Console ... 679
Registrazione degli eventi relativi ai dati con AWS Command Line Interface ... 689
Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati ... 702
Registrazione di eventi di dati per la conformità di AWS Config ... 714

Registrazione degli eventi relativi ai dati con AWS SDKs ... 715
Eventi di attività di rete ... 715
Campi avanzati di selezione degli eventi per gli eventi di attività di rete ... 717
Registrazione degli eventi relativi alle attività di rete con AWS Management Console ... 719
Registrazione degli eventi di attività di rete con AWS Command Line Interface ... 722
Registrazione degli eventi con AWS SDKs ... 745
Aggiungi chiavi di tag di risorsa e chiavi di condizione globali IAM agli eventi ... 745
Servizi AWS tag di risorse di supporto ... 747
Servizi AWS supporto delle chiavi di condizione globali IAM ... 748
Esempi di eventi ... 751
CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete ... 753
Ordine di troncamento dei campi per una dimensione massima dell'evento di 1 MB ... 767
Esempio di sharedEventID ... 767
CloudTrail registra contenuti per gli eventi Insights per i percorsi ... 768
Blocco `insightDetails` di esempio ... 773
CloudTrail registra i contenuti per gli eventi Insights per i datastore di eventi Lake. ... 776
CloudTrail elemento userIdentity ... 780
Esempi ... 781
Campi ... 782
Valori per AWS STS APIs con SAML e la federazione delle identità web ... 790
AWS STS identità di origine ... 792
Eventi non API acquisiti da CloudTrail ... 795
Servizio AWS eventi ... 795
AWS Management Console eventi di accesso ... 796
CloudTrail file di registro ... 812
Ricezione di file di CloudTrail registro da più regioni ... 814
Gestione della coerenza dei dati ... 815
Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs ... 816
Invio di eventi ai registri CloudWatch ... 817
Creazione CloudWatch di allarmi per CloudTrail eventi: esempi ... 825
Interruzione dell'invio CloudTrail di eventi ai registri CloudWatch ... 833
CloudWatch denominazione dei gruppi di log e dei flussi di log per CloudTrail ... 834
Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio ... 835
Ricezione di file di CloudTrail registro da più account ... 837

Redazione dell'account proprietario del bucket per gli eventi relativi ai dati richiamati da altri account IDs ... 838
Impostazione della policy del bucket per più account ... 839
Creazione di percorsi in account aggiuntivi ... 841
Condivisione di file di CloudTrail registro tra AWS account ... 843
Condivisione di file di log tra account tramite l'assunzione di un ruolo ... 844
Convalida dell'integrità dei file di CloudTrail registro ... 854
Perché usare questa funzionalità? ... 855
Come funziona ... 855
Abilitazione della convalida dell'integrità dei file di registro per CloudTrail ... 856
Convalida dell'integrità dei file di CloudTrail registro con AWS CLI ... 857
CloudTrail struttura del file digest ... 865
Implementazioni personalizzate della convalida dell'integrità dei file di CloudTrail registro ... 873
CloudTrail esempi di file di registro ... 885
CloudTrail formato del nome del file di registro ... 885
Esempi di file di log ... 886
Utilizzo della libreria CloudTrail di elaborazione ... 899
Requisiti minimi ... 899
Registri di elaborazione CloudTrail ... 899
Argomenti avanzati ... 905
Risorse aggiuntive ... 911
Sicurezza ... 912
Protezione dei dati ... 913
Identity and Access Management ... 914
Destinatari ... 915
Autenticazione con identità ... 915
Gestione dell'accesso con policy ... 919
Come AWS CloudTrail funziona con IAM ... 922
Esempi di policy basate su identità ... 931
Esempi di policy basate su risorse ... 948
Policy sui bucket Amazon S3 per CloudTrail ... 956
Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake ... 965
Policy tematica di Amazon SNS per CloudTrail ... 968
Risoluzione dei problemi ... 975
Uso di ruoli collegati ai servizi ... 979
AWS politiche gestite ... 986

Convalida della conformità 989
Resilienza 990
Sicurezza dell'infrastruttura 991
Prevenzione del problema "confused deputy" tra servizi 992
Best practice di sicurezza 992
CloudTrail best practice in materia di sicurezza investigativa 993
CloudTrail best practice di sicurezza preventiva 995
Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS) 999
Abilitazione della crittografia dei file di log 1000
Concessione delle autorizzazioni per la creazione di una chiave KMS 1002
Configura le politiche AWS KMS chiave per CloudTrail 1002
Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console 1018
Abilitazione e disabilitazione della crittografia per file di CloudTrail registro, file digest e archivi di dati di eventi con AWS CLI 1021
Come si AWS CloudTrail usa AWS KMS 1025
Cronologia dei documenti 1032
Aggiornamenti precedenti 1097
..... mcxviii

Che cos'è AWS CloudTrail?

AWS CloudTrail è uno strumento Servizio AWS che vi aiuta a consentire il controllo operativo e dei rischi, la governance e la conformità del vostro Account AWS. Le operazioni eseguite da un utente, un ruolo o un servizio AWS vengono registrate come eventi in CloudTrail. Gli eventi includono le azioni intraprese in AWS Management Console AWS Command Line Interface, e AWS SDKs e APIs.

CloudTrail offre tre modi per registrare gli eventi:

- Cronologia degli eventi: la cronologia degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli eventi di gestione verificatisi negli ultimi 90 giorni in una Regione AWS. Puoi cercare gli eventi filtrando gli eventi in base a un singolo attributo. Hai automaticamente accesso alla cronologia degli eventi quando crei il tuo account. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

  Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.
- CloudTrail Lake — AWS CloudTrail Lake è un data lake gestito per l'acquisizione, l'archiviazione, l'accesso e l'analisi delle attività degli utenti e delle API AWS per scopi di controllo e sicurezza. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili in base ai criteri selezionati applicando i selettori di eventi avanzati. Puoi conservare i dati degli eventi in un datastore di eventi per un massimo di 3.653 giorni (circa 10 anni) se scegli l'opzione Prezzo per la conservazione estendibile di un anno o di 2.557 giorni (circa 7 anni) se scegli l'opzione Prezzo per la conservazione di sette anni. È possibile creare un archivio dati di eventi per uno Account AWS o più eventi utilizzando. Account AWS AWS Organizations Puoi importare qualsiasi CloudTrail registro esistente dai tuoi bucket S3 in un data store di eventi esistente o nuovo. Puoi anche visualizzare le principali tendenze degli CloudTrail eventi con le dashboard di Lake. Per ulteriori informazioni, consulta Lavorare con AWS CloudTrail Lake.

  CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Quando si eseguono le query in Lake, si paga in base alla quantità di dati scansionati. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

- Percorsi: i percorsi registrano AWS le attività, distribuiscono e archiviano questi eventi in un bucket Amazon S3, con consegna opzionale a CloudWatch Logs e Amazon. EventBridge Puoi inserire questi eventi nelle tue soluzioni di monitoraggio della sicurezza. Puoi anche utilizzare soluzioni o soluzioni di terze parti come Amazon Athena per cercare e analizzare i tuoi CloudTrail log. Puoi creare percorsi singoli Account AWS o multipli Account AWS utilizzando. AWS OrganizationsÈ possibile registrare gli eventi di Insights per analizzare gli eventi di gestione alla ricerca di comportamenti anomali nella frequenza delle chiamate API e nei tassi di errore. Per ulteriori informazioni, consulta Creare un percorso per il tuo Account AWS.

  Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

La visibilità sull'attività AWS del tuo account è un aspetto chiave della sicurezza e delle migliori pratiche operative. Puoi utilizzarlo CloudTrail per visualizzare, cercare, scaricare, archiviare, analizzare e rispondere alle attività dell'account nell'intera AWS infrastruttura. Puoi identificare chi o cosa ha intrapreso quale azione, su quali risorse si è agito, quando si è verificato l'evento e altri dettagli per aiutarti ad analizzare e rispondere alle attività del tuo AWS account.

Puoi CloudTrail integrarti nelle applicazioni utilizzando l'API, automatizzare la creazione di data store di percorsi o eventi per la tua organizzazione, controllare lo stato degli archivi dati degli eventi e dei percorsi che crei e controllare il modo in cui gli utenti visualizzano gli CloudTrail eventi.

Accedendo CloudTrail

È possibile lavorare con CloudTrail in uno dei seguenti modi.

Argomenti

- CloudTrail console
- AWS CLI
- CloudTrail APIs
- AWS SDKs

CloudTrail console

Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.

La CloudTrail console fornisce un'interfaccia utente per l'esecuzione di molte CloudTrail attività come:

- Visualizzazione degli eventi recenti e della cronologia degli eventi per il tuo AWS account.
- Scaricamento di un file filtrato o completo degli ultimi 90 giorni di gestione degli eventi dalla cronologia degli eventi.
- Creazione e modifica di CloudTrail percorsi.
- Creazione e modifica di archivi di dati di eventi CloudTrail Lake.
- Esecuzione di query sugli archivi di dati degli eventi.
- Configurazione dei CloudTrail percorsi, tra cui:
  - Selezione di un bucket Amazon S3 per i trail.
  - Impostazione di un prefisso.
  - Configurazione della consegna nei registri. CloudWatch
  - Utilizzo AWS KMS delle chiavi per la crittografia dei dati delle tracce.
  - Abilitazione delle notifiche Amazon SNS per la distribuzione dei file di log ai trail.
  - Aggiunta e gestione dei tag per i trail.
- Configurazione degli archivi di dati di eventi CloudTrail Lake, tra cui:
  - Integrazione degli archivi di dati sugli eventi con CloudTrail i partner o con le proprie applicazioni, per registrare eventi da fonti esterne. AWS
  - Federazione degli archivi di dati di eventi per eseguire query da Amazon Athena.
  - Utilizzo di AWS KMS chiavi per la crittografia dei dati del data store degli eventi.
  - Aggiunta e gestione dei tag per gli archivi di dati degli eventi.

Per ulteriori informazioni su AWS Management Console, vedere AWS Management Console.

AWS CLI

AWS Command Line Interface È uno strumento unificato con cui è possibile interagire CloudTrail dalla riga di comando. Per ulteriori informazioni, consulta la AWS Command Line Interface Guida per

l'utente di . Per un elenco completo dei comandi CloudTrail CLI, consulta cloudtrail e cloudtrail-data nel Command Reference.AWS CLI

CloudTrail APIs

Oltre alla console e alla CLI, puoi anche utilizzare CloudTrail RESTful APIs per programmare CloudTrail direttamente. Per ulteriori informazioni, consulta l'AWS CloudTrail API Reference e il CloudTrail-Data API Reference.

AWS SDKs

In alternativa all'utilizzo dell' CloudTrail API, puoi utilizzare uno dei AWS SDKs. Ogni SDK include librerie e codice di esempio per piattaforme e linguaggi di programmazione diversi. SDKs Forniscono un modo conveniente per creare un accesso programmatico a CloudTrail. Ad esempio, è possibile utilizzare il SDKs per firmare le richieste in modo crittografico, gestire gli errori e riprovare automaticamente le richieste. Per ulteriori informazioni, consulta la pagina Strumenti per creare. AWS

Come CloudTrail funziona

Hai automaticamente accesso alla cronologia degli CloudTrail eventi quando crei il tuo Account AWS. La cronologia degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli eventi di gestione verificatisi negli ultimi 90 giorni in una Regione AWS.

Per una registrazione continua degli eventi nell' Account AWS oltre i 90 giorni, creare un trail o un datastore di eventi CloudTrail Lake.

Argomenti

- CloudTrail Cronologia degli eventi
- CloudTrail Archivi di dati dei laghi e degli eventi
- CloudTrail Cruscotti di Lake
- CloudTrail sentieri
- CloudTrail Eventi Insights
- CloudTrail canali

CloudTrail Cronologia degli eventi

Puoi visualizzare facilmente gli ultimi 90 giorni di eventi di gestione nella CloudTrail console accedendo alla pagina Cronologia degli eventi. È inoltre possibile visualizzare la cronologia degli eventi eseguendo il comando aws cloudtrail lookup-events o l'operazione API `LookupEvents`. Puoi cercare gli eventi in Event history (Cronologia degli eventi) filtrando gli eventi in base a un singolo attributo. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

La cronologia degli eventi non è collegata ai percorsi o ai datastore di eventi presenti nel tuo account e non è interessata dalle modifiche alla configurazione apportate ai percorsi e ai datastore di eventi.

Non sono CloudTrail previsti costi per la visualizzazione della pagina della cronologia degli eventi o l'esecuzione del `lookup-events` comando.

CloudTrail Archivi di dati dei laghi e degli eventi

È possibile creare un archivio dati di eventi per registrare CloudTrail eventi (eventi di gestione, eventi relativi ai dati, eventi di attività di rete), eventi CloudTrail Insights, AWS Audit Manager prove, elementi di AWS Config configurazione o eventi esterni a AWS.

I datastore di eventi possono registrare eventi dalla corrente Regione AWS o da tutte le Regioni AWS del tuo AWS account. I datastore di eventi utilizzati per registrare gli eventi di integrazione dall'esterno di AWS devono riguardare solo una singola Regione; i datastore di eventi non possono riferirsi a più Regioni.

Se hai creato un'organizzazione in AWS Organizations, puoi creare un archivio di dati degli eventi dell'organizzazione che registri tutti gli eventi per tutti gli AWS account dell'organizzazione. Gli archivi di dati degli eventi dell'organizzazione possono applicarsi a tutte le Regioni AWS o alla Regione corrente. I datastore di eventi dell'organizzazione devono essere creati nell'account di gestione o nell'account dell'amministratore delegato e, se specificati come applicabili a un'organizzazione, vengono applicati automaticamente a tutti gli account membri di tale organizzazione. Gli account membri possono visualizzare l'archivio di dati degli eventi dell'organizzazione, ma non possono modificarlo o eliminarlo. Gli archivi di dati degli eventi dell'organizzazione non possono essere utilizzati per raccogliere eventi dall'esterno di AWS. Per ulteriori informazioni, consulta Comprendere gli archivi di dati degli eventi organizzativi.

Per impostazione predefinita, tutti gli eventi in un datastore di eventi sono crittografati da CloudTrail. Quando configuri un datastore di eventi, puoi scegliere di utilizzare il tuo AWS KMS key. L'utilizzo della tua chiave KMS comporta AWS KMS costi di per la crittografia e la decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o

modificata. Per ulteriori informazioni, consulta Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS).

La seguente tabella fornisce informazioni sulle operazioni che è possibile eseguire sui datastore di eventi.

Attività	Descrizione
Visualizza e crea dashboard	Puoi utilizzare le dashboard di CloudTrail Lake per visualizz are le tendenze degli eventi per gli archivi di dati sugli eventi presenti nel tuo account. Puoi visualizzare dashboard gestite, creare dashboard personalizzate e abilitare la dashboard Highlights per visualizzare i momenti salienti dei dati sugli eventi curati e gestiti da Lake. CloudTrail
Registra gli eventi di gestione	Configurare il datastore di eventi in modo che registrino gli eventi di sola lettura, gli eventi di sola lettura o tutti gli eventi di gestione. Per impostazione predefinita, i datastore di eventireg istrano gli eventi di gestione dei log. È possibile filtrare gli eventi di gestione nei seguenti campi avanzati di selezione degli eventi: `eventName` `eventSour ce` ,`eventType` ,, `readOnlysessionCredentialF romConsole` , `euserIdentity.arn` .
Registra gli eventi relativi ai dati	È possibile utilizzare selettori di eventi avanzati per creare selettori dettagliati per registrare solo gli eventi di dati di interesse. Ad esempio, puoi filtrare in base al `eventName` campo per includere o escludere la registrazione di chiamate API specifiche, il che può aiutare a controllare i costi. Per ulteriori informazioni, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.
Registra gli eventi delle attività di rete	Configurare il datastore di eventi in modo che registrino gli eventi di attività di rete. È possibile utilizzare selettori di eventi avanzati per filtrare in base ai `vpcEndpointId` campi `eventName` `errorCode` , e per registrare solo gli eventi di interesse.

Attività	Descrizione
Eventi di Log Insights	Configurare i datastore di eventi in modo che registrino gli eventi Insights per individuare e rispondere ad attività insolite associate alle chiamate API di gestione. Per ulteriori informazioni, consulta Lavorare con CloudTrail Insights. Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail.
Copia gli eventi del percorso	Puoi copiare gli eventi del percorso in un datastore di eventi nuovo o in uno esistente per creare uno point-in-time snapshot degli eventi registrati nel percorso.
Abilitazione della federazione in un datastore di eventi	Puoi eseguire la federazione di un datastore di eventi per visualizzare i metadati associati al datastore nel Catalogo AWS Glue dati ed eseguire query SQL sui dati degli eventi utilizzando Amazon Athena. I metadati della tabella archiviati nel Catalogo AWS Glue dati consentono al motore di query Athena di trovare, leggere ed elaborare i dati su cui desideri eseguire query.
Interruzione o avvio dell'acquisizione di eventi su un datastore di eventi	È possibile interrompere e avviare l'acquisizione di eventi su datastore di eventi che raccolgono eventi di CloudTrail gestione e dati o elementi di AWS Config configurazione.
Creazione di un'integrazione con un'origine di eventi esterna ad AWS	Puoi utilizzare le integrazioni di CloudTrail Lake per registrare e archiviare i dati delle attività degli utenti dall'esterno di AWS, da qualsiasi origine nei tuoi ambienti ibridi, ad esempio applicazioni interne o SaaS ospitate on-premise o nel cloud, macchine virtuali o container. Per informazioni sui partner di integrazione disponibili, consulta Lake Integrations.AWS CloudTrail
Visualizzazione delle query di esempio di Lake nella console CloudTrail	La CloudTrail console fornisce una serie di query di esempio che possono esserti utili per iniziare a scrivere le tue query.

Attività	Descrizione
Creare o modificare un'interrogazione	Le query in CloudTrail sono scritte in SQL. È possibile creare una query nella scheda Editor di CloudTrail Lake scrivendo la query in SQL partendo da zero o aprendo una query salvata o di esempio e modificandola.
Salvataggio dei risultati della query in un bucket S3	Quando si esegue una query, è possibile salvare i risultati della query in un bucket S3.
Scaricare i risultati della query salvati	È possibile scaricare un file CSV contenente i risultati della query di CloudTrail Lake salvati.
Convalida dei risultati della query salvati	Per determinare se i risultati della CloudTrail query sono stati modificati, eliminati o non modificati dopo che sono stati CloudTrail distribuiti i risultati della query al bucket S3, è possibile utilizzare la funzionalità di convalida dell'integrità dei risultati della query.

Per ulteriori informazioni su CloudTrail Lake, consulta. Lavorare con AWS CloudTrail Lake

CloudTrail I datastore di eventi e le query di Data Lake comportano addebiti. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Quando si eseguono le query in Lake, si paga in base alla quantità di dati scansionati. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, consulta AWS CloudTrail Prezzi di eGestione dei costi CloudTrail del lago.

CloudTrail Cruscotti di Lake

Puoi utilizzare le dashboard di CloudTrail Lake per visualizzare le tendenze degli eventi per gli archivi di dati sugli eventi presenti nel tuo account. CloudTrail Lake offre i seguenti tipi di pannelli di controllo:

- Dashboard gestiti: puoi visualizzare un dashboard gestito per visualizzare le tendenze degli eventi per un datastore di eventi che raccoglie eventi di gestione, eventi di dati o eventi Insights. Queste dashboard sono automaticamente disponibili per te e sono gestite da Lake. CloudTrail CloudTrail offre 14 dashboard gestite tra cui scegliere. Puoi aggiornare manualmente i dashboard gestiti. Non è possibile modificare, aggiungere o rimuovere i widget per questi dashboard, tuttavia, è possibile

salvare un dashboard gestito come dashboard personalizzato se si desidera modificare i widget o impostare una pianificazione di aggiornamento.

- Dashboard personalizzati: i dashboard personalizzati consentono di interrogare gli eventi in qualsiasi tipo di archivio dati di eventi. Puoi aggiungere fino a 10 widget a un pannello di controllo personalizzato. Puoi aggiornare manualmente una dashboard personalizzata oppure impostare una pianificazione di aggiornamento.
- Dashboard Highlights: abilita la dashboard Highlights per visualizzare una at-a-glance panoramica dell' AWS attività raccolta dagli archivi di dati sugli eventi presenti nel tuo account. La dashboard Highlights è gestita CloudTrail e include widget pertinenti al tuo account. I widget mostrati nella dashboard Highlights sono unici per ogni account. Questi widget potrebbero far emergere attività o anomalie rilevate. Ad esempio, la dashboard Highlights potrebbe includere il widget Total cross-account access, che mostra se c'è un aumento delle attività anomale tra account. CloudTrail aggiorna la dashboard Highlights ogni 6 ore. La dashboard mostra i dati delle ultime 24 ore dall'ultimo aggiornamento.

Ogni tipo di pannello di controllo è composto da uno o più widget rappresenta una query SQL.

Per ulteriori informazioni, consulta CloudTrail Cruscotti Lake.

CloudTrail sentieri

Un trail è una configurazione che abilita la distribuzione di eventi in un bucket Amazon S3 che specifichi. Puoi anche fornire e analizzare gli eventi in un percorso con Amazon CloudWatch Logs e Amazon EventBridge.

I percorsi possono registrare eventi di CloudTrail gestione, eventi di attività di rete ed eventi Insights.

Puoi creare percorsi multiregione e a regione singola per i tuoi. Account AWS

Percorsi multi-regione

Quando crei un percorso multiregionale, CloudTrail registra gli eventi in tutti Regioni AWS gli elementi abilitati nel tuo Account AWS e distribuisce i file di log CloudTrail degli eventi in un bucket S3 specificato. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multi-regione. È possibile convertire un trail per una singola Regione in un percorso multi-regione utilizzando la. AWS CLI Per ulteriori informazioni, consulta Comprendere i percorsi multiregionali e le regioni opt-in, Creazione di un percorso con la console e Conversione di un percorso a regione singola in un percorso multiregionale.

Percorsi a regione singola

Quando crei un trail per una singola Regione, CloudTrail registra solo gli eventi in quella Regione. Distribuisce quindi i file di log CloudTrail degli eventi a un bucket Amazon S3 specificato. Puoi creare un percorso basato su una singola Regione solo utilizzando la AWS CLI. Se crei altri percorsi singoli, puoi configurarli in modo che distribuiscano i file di log CloudTrail degli eventi nello stesso bucket S3 o in bucket distinti. Questa è l'opzione predefinita quando crei un percorso utilizzando la AWS CLI o l' CloudTrail API. Per ulteriori informazioni, consulta Creazione, aggiornamento e gestione di percorsi con AWS CLI.

> **Note**
>
> Per entrambi i tipi di percorsi, puoi specificare un bucket Amazon S3 di qualsiasi Regione.

Se hai creato un'organizzazione in AWS Organizations, puoi creare un trail dell'organizzazione che registri tutti gli eventi per tutti gli AWS account dell'organizzazione. I percorsi dell'organizzazione possono essere applicati a tutte le AWS Regioni o alla Regione corrente. I percorsi dell'organizzazione devono essere creati nell'account di gestione o nell'account dell'amministratore delegato e, se specificati come applicabili a un'organizzazione, vengono applicati automaticamente a tutti gli account membri dell'organizzazione. Gli account membri possono visualizzare il trail dell'organizzazione, ma non possono modificarlo o eliminarlo. Per impostazione predefinita, gli account membro non hanno accesso ai file di log del trail dell'organizzazione nel bucket Amazon S3.

Per impostazione predefinita, quando crei un percorso nella CloudTrail console, i file di log degli eventi e i file digest sono crittografati con una chiave KMS. Se scegli di non abilitare la crittografia SSE-KMS, i file di log degli eventi e i file digest vengono crittografati utilizzando la crittografia lato server (SSE) di Amazon S3. Puoi archiviare i file di log nel tuo bucket per la durata desiderata. Puoi anche definire regole del ciclo di vita di Amazon S3 per archiviare o eliminare file di log automaticamente. Se desideri ricevere notifiche relative alla distribuzione e alla convalida dei file di log, puoi configurare le notifiche Amazon SNS.

CloudTrail pubblica i file di log più volte in un'ora, circa ogni cinque minuti. Questi file di log contengono le chiamate API dai servizi nell'account che supportano CloudTrail. Per ulteriori informazioni, consulta CloudTrail servizi e integrazioni supportati.

> **Note**
>
> CloudTrail in genere distribuisce i log con una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail.
>
> Se configuri erroneamente il percorso (ad esempio, il bucket S3 è irraggiungibile), CloudTrail tenterà di inviare di nuovo i file di log al bucket S3 per 30 giorni e per questi attempted-to-deliver tentativi di invio saranno applicati i costi standard. CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.
>
> CloudTrail acquisisce le operazioni eseguite direttamente dall'utente o per conto dell'utente da un AWS servizio. Ad esempio, una AWS CloudFormation `CreateStack` chiamata può generare altre chiamate API ad Amazon EC2, Amazon RDS, Amazon EBS o altri servizi, secondo quanto stabilito dal AWS CloudFormation modello. Questo comportamento è normale e previsto. Puoi capire se l'azione è stata eseguita da un AWS servizio utilizzando il `invokedby` campo nell' CloudTrailevento.

La seguente tabella fornisce informazioni sulle operazioni che è possibile eseguire sui percorsi.

Attività	Descrizione
Registrazione degli eventi di gestione	Configurare i trail in modo che registrino gli eventi di sola lettura, gli eventi di sola lettura o tutti gli eventi di gestione.
Registra gli eventi relativi ai dati	È possibile utilizzare selettori di eventi avanzati per creare selettori dettagliati per registrare solo gli eventi di dati di interesse. Ad esempio, puoi filtrare in base al `eventName` campo per includere o escludere la registrazione di chiamate API specifiche, il che può aiutare a controllare i costi. Per ulteriori informazioni, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.
Registra gli eventi delle attività di rete	Configura i tuoi percorsi per registrare gli eventi delle attività di rete. È possibile configurare

Attività	Descrizione
	selettori di eventi avanzati per filtrare in base ai `vpcEndpointId` campi `eventName` `errorCode` , e per registrare solo gli eventi di interesse.
Eventi di Log Insights	Configurare i percorsi in modo che registrino gli eventi Insights per aiutare a individuare e a rispondere ad attività insolite associate con chiamate API di gestione . Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.
Visualizza gli eventi di Insights	Dopo aver abilitato CloudTrail Insights su un percorso, puoi visualizzare fino a 90 giorni di eventi Insights utilizzando la CloudTrail console o la AWS CLI.
Scarica gli eventi Insights	Dopo aver abilitato CloudTrail Insights su un percorso, puoi scaricare un file CSV o JSON contenente fino agli ultimi 90 giorni di eventi Insights per il percorso.
Copia eventi traccia su CloudTrail Lake	Puoi copiare gli eventi traccia esistenti in un archivio dati degli eventi CloudTrail Lake per creare una point-in-time snapshot degli eventi registrati nel percorso.

Attività	Descrizione
Creazione e iscrizione a un argomento Amazon SNS	Esegui la sottoscrizione a un argomento per ricevere le notifiche relative alla distribuzione dei file di log nel bucket. Amazon SNS può inviare notifiche in diversi modi, ad esempio a livello di programmazione con Amazon Simple Queue Service. **Note** Se si desidera ricevere notifiche SNS relative alle distribuzioni dei file di log da tutte le Regioni, specificare un solo argomento SNS per il percorso. Se si desidera elaborare tutti gli eventi a livello di programmazione, consultar e Utilizzo della libreria CloudTrail di elaborazione.
Visualizza i tuoi file di log	Trova e scarica i tuoi file di registro dal bucket S3.
Monitora gli eventi con Logs CloudWatch	È possibile configurare il percorso in modo che inviino gli eventi ai CloudWatch log. È possibile quindi utilizzare CloudWatch Logs per monitorare l'account per chiamate API ed eventi specifici. **Note** Se si configura un percorso multiregi onale per l'invio di eventi a un gruppo di log di CloudWatch log di log, CloudTrai l invia gli eventi provenienti da tutte le Regioni a un unico gruppo di log.

Attività	Descrizione
Abilita la crittografia SSE-KMS	La crittografia dei file di log e dei file digest con una chiave KMS fornisce un ulteriore livello di sicurezza per i dati. CloudTrail
Abilitazione dell'integrità dei file di log	La convalida dell'integrità dei file di log consente di verificare che i file di log siano rimasti invariati da quando sono stati CloudTrai l distribuiti.
Condividi i file di registro con altri Account AWS	È possibile condividere i file di log tra account.
Registri aggregati di più account	È possibile aggregare i file di log da più account in un unico bucket.
Collabora con le soluzioni dei partner	Analizzare i CloudTrail risultati con una soluzione partner integrata in. CloudTrail Le soluzioni di partner offrono un'ampia gamma di funzionalità, ad esempio il rilevamento delle modifiche, la risoluzione dei problemi e l'analisi della sicurezza.

Puoi fornire gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket S3 CloudTrail creando un percorso, tuttavia dovranno essere considerati i costi di archiviazione di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Eventi Insights

AWS CloudTrail Insights aiuta AWS gli utenti a identificare e a rispondere ad attività insolite o anomale associate alla frequenza delle chiamate API e di errore API grazie a un'analisi continua degli eventi di CloudTrail gestione. CloudTrail Insights analizza i modelli normali del volume delle chiamate API e i tassi di errore API, chiamati anche riferimento, e genera eventi Insights quando il volume delle chiamate o la frequenza di errore sono al di fuori dei modelli normali. Gli eventi di Insights sulla frequenza delle chiamate API vengono generati per la `write` gestione APIs e gli eventi Insights sulla frequenza di errore API vengono generati per entrambi `read` APIs. `write`

Per impostazione predefinita, i CloudTrail percorsi e i datastore di eventi non registrano gli eventi Insights. È necessario configurare il datastore di eventi o eventi per registrare gli eventi Insights. Per ulteriori informazioni, consultare Registrazione degli eventi di Insights con la console CloudTrail e Registrazione degli eventi di Insights con AWS CLI.

Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Visualizzazione di eventi Insights per percorsi e archivi di dati degli eventi

CloudTrail supporta gli eventi Insights sia per i percorsi che per i datastore di eventi, tuttavia esistono alcune differenze nel modo in cui si visualizzano e si accede agli eventi Insights.

Visualizzazione di eventi Insights per i percorsi

Se hai abilitato gli eventi Insights su un percorso e CloudTrail rileva un'attività insolita, gli eventi Insights vengono registrati in una cartella diversa, o prefisso, nel bucket S3 di destinazione del tuo percorso. Puoi anche visualizzare il tipo di informazioni dettagliate e il periodo di tempo dell'incidente quando visualizzi gli eventi Insights nella CloudTrail console. Per ulteriori informazioni, consulta Visualizzazione degli eventi Insights per i percorsi con la console.

Dopo che hai abilitato CloudTrail Insights per la prima volta su un percorso, CloudTrail potrebbe essere necessario attendere fino a 36 ore per iniziare a fornire gli eventi Insights dopo che hai abilitato gli eventi Insights su un percorso, a condizione che venga rilevata un'attività insolita durante tale periodo.

Visualizzazione degli eventi Insights per i datastore di eventi

Per registrare gli eventi di Insights in CloudTrail Lake, è necessario un datastore di eventi di destinazione che registri gli eventi Insights e un datastore di eventi di origine che abiliti Insights e registri gli eventi di gestione. Per ulteriori informazioni, consulta Crea un archivio dati sugli eventi per gli eventi Insights con la console.

Dopo che hai abilitato CloudTrail Insights per la prima volta nel datastore di eventi di origine, CloudTrail potrebbe essere necessario attendere fino a 7 giorni affinché venga rilevata un'attività insolita durante tale periodo.

Se hai abilitato CloudTrail Insights in un archivio dati degli eventi di origine e CloudTrail rileva un'attività insolita, CloudTrail distribuisce gli eventi Insights al datastore di eventi di destinazione. Puoi

quindi interrogare il datastore di eventi di destinazione per ottenere informazioni sugli eventi Insights e, facoltativamente, salvare i risultati della query in un bucket S3. Per ulteriori informazioni, consultare Crea o modifica un'interrogazione con la console CloudTrail e Visualizza query di esempio con la console CloudTrail .

È possibile visualizzare il pannello di controllo degli eventi Insights per visualizzare gli eventi Insights nell'archivio di dati degli eventi di destinazione. Per ulteriori informazioni sui pannelli di controllo di Lake, consulta CloudTrail Cruscotti Lake.

CloudTrail canali

CloudTrail supporta due tipi di canali:

Canali per le integrazioni di CloudTrail Lake con origini di eventi esterne ad. AWS

CloudTrail Lake utilizza i canali per importare eventi dall'esterno di AWS CloudTrail Lake da partner esterni che collaborano con CloudTrail o da origini di tua proprietà. Quando crei un canale, scegli uno o più archivi di dati degli eventi per archiviare gli eventi che provengono dall'origine del canale. È possibile modificare gli archivi di dati degli eventi di destinazione per un canale in base alle esigenze, a condizione che tali archivi siano impostati per registrare gli eventi dell'attività. Quando crei un canale per gli eventi provenienti da un partner esterno, fornisci un ARN di canale al partner o all'applicazione di origine. La policy delle risorse collegata al canale consente all'origine di trasmettere eventi attraverso il canale. Per ulteriori informazioni, consulta le pagine Crea un'integrazione con una fonte di eventi esterna a AWS e `CreateChannel` nella Documentazione di riferimento dell'API AWS CloudTrail .

Canali collegati al servizio

AWS I servizi possono creare un canale collegato ai servizi per ricevere CloudTrail eventi per tuo conto. Il AWS servizio che crea il canale collegato ai servizi configura selettori di eventi avanzati per il canale e specifica se il canale si applica a tutte le Regioni o a una singola Regione.

È possibile utilizzare la CloudTrail console o visualizzare informazioni su qualsiasi AWS CLI CloudTrail canale collegato al servizio creato da. Servizi AWS

CloudTrail concetti

Questa sezione riassume i concetti di base relativi a CloudTrail.

Concetti:

- CloudTrail eventi
- Cronologia degli eventi
- Trail
- Percorsi organizzativi
- CloudTrail Archivi di dati su laghi ed eventi
- CloudTrail Approfondimenti
- Tag
- AWS Security Token Service e CloudTrail
- Eventi dei servizi globali

CloudTrail eventi

Un evento in CloudTrail è la registrazione di un'attività in un AWS account. Questa attività può essere un'azione intrapresa da un'identità IAM o da un servizio monitorabile da CloudTrail. CloudTrailgli eventi forniscono una cronologia delle attività dell'account API e non API effettuate tramite gli AWS Management Console strumenti a riga di comando e altri AWS servizi. AWS SDKs

CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

CloudTrail registra quattro tipi di eventi:

- Eventi di gestione
- Eventi di dati
- Eventi di attività di rete
- Eventi di approfondimento

Tutti i tipi di eventi utilizzano un formato di registro CloudTrail JSON.

Per impostazione predefinita, i percorsi e i datastore di eventi registrano gli eventi di gestione, ma non gli eventi di dati o gli eventi Insights.

Per informazioni su come effettuare l' Servizi AWS integrazione con CloudTrail, consultaAWS argomenti di servizio per CloudTrail.

Eventi di gestione

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse AWS dell'account. Queste operazioni sono definite anche operazioni del piano di controllo.

Gli eventi di gestione di esempio includono:

- Configurazione della sicurezza (ad esempio, operazioni AWS Identity and Access Management `AttachRolePolicy` API).
- Registrazione di dispositivi (ad esempio, operazioni EC2 `CreateDefaultVpc` API Amazon).
- Configurazione delle regole per il routing dei dati (ad esempio, le operazioni delle EC2 `CreateSubnet` API Amazon).
- Configurazione della registrazione (ad esempio, operazioni AWS CloudTrail `CreateTrail` API).

Gli eventi di gestione possono includere anche eventi non API che si verificano nel tuo account. Ad esempio, quando un utente accede al tuo account, CloudTrail registra l'`ConsoleLogin`evento. Per ulteriori informazioni, consulta Eventi non API acquisiti da CloudTrail.

Per impostazione predefinita, CloudTrail trails and CloudTrail Lake Event Data archivia gli eventi di gestione dei registri. Per ulteriori informazioni sulla gestione della registrazione degli eventi, vedereRegistrazione degli eventi di gestione.

Eventi di dati

Gli eventi di dati forniscono informazioni sulle operazioni eseguite in una risorsa o al suo interno. Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati.

Gli eventi di dati di esempio includono:

- Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject``DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket S3.
- AWS Lambda attività di esecuzione della funzione (l'API). `Invoke`
- CloudTrail `PutAuditEvents`attività su un canale CloudTrail Lake che viene utilizzata per registrare eventi dall'esterno AWS.
- Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.

La tabella seguente mostra i tipi di risorse disponibili per i percorsi e gli archivi di dati di eventi. La colonna Tipo di risorsa (console) mostra la selezione appropriata nella console. La colonna del valore resources.type mostra il `resources.type` valore da specificare per includere eventi di dati di quel tipo nel tuo trail o event data store utilizzando o. AWS CLI CloudTrail APIs

Per i trail, puoi utilizzare selettori di eventi di base o avanzati per registrare gli eventi di dati per oggetti Amazon S3 in bucket generici, funzioni Lambda e tabelle DynamoDB (mostrate nelle prime tre righe della tabella). Puoi utilizzare solo selettori di eventi avanzati per registrare i tipi di risorse mostrati nelle righe rimanenti.

Per i datastore di eventi, per includere gli eventi di dati è possibile utilizzare solo i selettori di eventi avanzati.

Eventi di dati supportati da AWS CloudTrail

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Backup	AWS Backup Attività dell'API Search Data sulle offerte di lavoro di ricerca.	AWS Backup Dati di ricerca APIs	`AWS::Backup::SearchJob`
AWS IoT	AWS IoT Attività delle API sui certificati.	Certificato IoT	`AWS::IoT::Certificate`
AWS IoT	AWS IoT Attività delle API sugli oggetti.	Cosa IoT	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Connettore per l'attività dell'API di Active Directory.	AWS Private CA Connettore per Active Directory	`AWS::PCAConnectorAD::Connector`
AWS Private CA	AWS Private CA Connettore per l'attività dell'API SCEP.	AWS Private CA Connettore per SCEP	`AWS::PCAConnectorSCEP::Connector`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon RDS	Attività dell'API Amazon RDS su un cluster DB.	API dati RDS - Cluster DB	`AWS::RDS::DBCluster`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject`, e operazioni `PutObject` API) su oggetti in bucket generici.	S3	`AWS::S3::Object`
Amazon S3	Attività dell'API Amazon S3 sui punti di accesso.	Punto di accesso S3	`AWS::S3::AccessPoint`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket di directory.	S3 Express	`AWS::S3Express::Object`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon S3	Attività delle API dei punti di accesso Amazon S3 Object Lambda, ad esempio chiamate a e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	Attività FSx delle API Amazon sui volumi.	FSx Volume	`AWS::FSx::Volume`
Tabelle di Amazon S3	Attività dell'API Amazon S3 sulle tabelle.	Tabella S3	`AWS::S3Tables::Table`
Tabelle di Amazon S3	Attività dell'API Amazon S3 su bucket da tabella.	Secchio da tavolo S3	`AWS::S3Tables::TableBucket`
Amazon S3 su Outposts	Attività dell'API a livello di oggetto di Amazon S3 su Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SNS	Operazioni dell'API `Publish` Amazon SNS sugli endpoint della piattaforma.	Endpoint della piattaforma SNS	`AWS::SNS::PlatformEndpoint`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon SNS	Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.	Argomento SNS	`AWS::SNS::Topic`
Amazon SQS	Attività dell'API Amazon SQS sui messaggi.	SQS	`AWS::SQS::Queue`
Catena di approvvigionamento di AWS	Catena di approvvigionamento di AWS Attività dell'API su un'istanza.	Catena di fornitura	`AWS::SCN::Instance`
Amazon SWF	Attività dell'API Amazon SWF sui domini.	Dominio SWF	`AWS::SWF::Domain`
AWS AppConfig	AWS AppConfig Attività dell'API per operazioni di configurazione come chiamate a `StartConfigurationSessioneGetLatestConfiguration`.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AWS AppSync Attività delle API su AppSync GraphQL APIs.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Aurora DSQL	Attività dell'API SQL di Amazon Aurora sulle risorse del cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
AWS Scambio di dati B2B	Attività dell'API Scambio di dati B2B per operazioni Transformer, come le chiamate a `GetTransformerJob` e `StartTransformerJob` .	Scambio di dati B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Attività dell'API Amazon Bedrock sull'alias di un agente.	Alias dell'agente Bedrock	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle chiamate asincrone.	Richiamo asincrono Bedrock	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	Attività dell'API Amazon Bedrock su un alias di flusso.	Alias di flusso Bedrock	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui guardrail.	Parapetto Bedrock	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Attività dell'API Amazon Bedrock sugli agenti in linea.	Agente in linea Bedrock Invoke	`AWS::Bedrock::InlineAgent`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Bedrock	Attività dell'API Amazon Bedrock su una knowledge base.	Knowledge base Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui modelli.	Modello Bedrock	`AWS::Bedrock::Model`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui prompt.	Richiesta Bedrock	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	Attività dell'API Amazon Bedrock nelle sessioni.	Sessione Bedrock	`AWS::Bedrock::Session`
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle esecuzioni dei flussi.	Esecuzione del flusso di base	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una politica di ragionamento automatico.	Politica di ragionamento automatizzato di base	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una versione di policy di ragionamento automatico.	Versione della politica di ragionamento automatizzato di Bedrock	`AWS::Bedrock::AutomatedReasoningPolicyVersion`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Cloud Map	AWS Cloud Map Attività dell'API su un namespace.	AWS Cloud Map spazio dei nomi	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	AWS Cloud Map Attività dell'API su un servizio.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	CloudFront Attività delle API su un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS CloudTrail	CloudTrail `PutAuditEvents` attività su un canale CloudTrail Lake che viene utilizzato per registrare eventi dall'esterno AWS.	CloudTrail canale	`AWS::CloudTrail::Channel`
Amazon CloudWatch	Attività dell' CloudWatch API Amazon sulle metriche.	CloudWatch parametro	`AWS::CloudWatch::Metric`
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sui monitor.	Monitor di Network Flow Monitor	`AWS::NetworkFlowMonitor::Monitor`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sugli ambiti.	Ambito di Network Flow Monitor	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	Attività dell'API Amazon CloudWatch RUM sui monitor delle app.	Monitoraggio delle app RUM	`AWS::RUM::AppMonitor`
Amazon CodeGuru Profiler	CodeGuru Attività dell'API Profiler sui gruppi di profilazione.	CodeGuru Gruppo di profilazione Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su una personalizzazione.	CodeWhisperer personalizzazione	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su un profilo.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Attività dell'API Amazon Cognito sui pool di identità di Amazon Cognito.	Pool di identità di Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange Attività delle API sugli asset.	Risorsa Data Exchange	`AWS::DataExchange::Asset`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Deadline Cloud	Deadline CloudAttività delle API sulle flotte.	Deadline Cloud flotta	`AWS::Deadline::Fleet`
AWS Deadline Cloud	Deadline Cloudattività delle API sui lavori.	Deadline Cloud lavoro	`AWS::Deadline::Job`
AWS Deadline Cloud	Deadline Cloudattività delle API in coda.	Deadline Cloud coda	`AWS::Deadline::Queue`
AWS Deadline Cloud	Deadline CloudAttività delle API sui lavoratori.	Deadline Cloud lavoratore	`AWS::Deadline::Worker`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon DynamoDB	Attività delle API a livello di elemento di Amazon DynamoDB sulle tabelle (ad esempio `PutItem`, `DeleteItem` e operazioni API). `UpdateItem` **Note** Per le tabelle con flussi abilitati, il campo `resources` nell'evento di dati contiene sia `AWS::DynamoDB::Stream` che `AWS::DynamoDB::Table`. Se specifichi `AWS::DynamoDB::Table` come `resources.type`, per impostazione predefini	DynamoDB	`AWS::DynamoDB::Table`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
	ta verranno registrati sia gli eventi della tabella DynamoDB che quelli dei flussi DynamoDB. Per escludere gli eventi di streaming, aggiungi un filtro sul campo. `eventName`		
Amazon DynamoDB	Attività dell'API Amazon DynamoDB sui flussi	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct APIs, ad esempio `GetSnapshotBlock` e su `PutSnapshotBlock` istantanee e `ListChangedBlocks` Amazon EBS.	Amazon EBS diretto APIs	`AWS::EC2::Snapshot`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Elastic Kubernetes Service	Attività dell'API Amazon Elastic Kubernetes Service sulle dashboard.	Pannello di controllo di Amazon Elastic Kubernetes Service	`AWS::EKS::Dashboard`
Amazon EMR	Attività dell'API Amazon EMR su un'area di lavoro di log write-ahead.	Workspace di registrazione write-ahead EMR	`AWS::EMRWAL::Workspace`
AWS Messaggistica per l'utente finale (SMS)	AWS Attività dell'API SMS di messaggistica per l'utente finale sulle identità di origine.	Identità di origine tramite SMS Voice	`AWS::SMSVoice::OriginationIdentity`
AWS SMS di messaggistica per l'utente finale	AWS Attività dell'API SMS di messaggistica per l'utente finale sui messaggi.	Messaggio vocale SMS	`AWS::SMSVoice::Message`
AWS Messaggistica sociale per utenti finali	AWS Attività dell'API Social Messaging per l'utente finale sul numero di telefono IDs.	ID del numero di telefono di messaggistica sociale	`AWS::SocialMessaging::PhoneNumberId`
AWS Social di messaggistica per utenti finali	AWS Attività dell'API End User Messaging Social su Waba IDs.	ID Waba per la messaggistica sociale	`AWS::SocialMessaging::WabaId`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon FinSpace	Attività dell'API Amazon FinSpace sugli ambienti	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Stream	L'attività delle API di streaming di Amazon GameLift Streams sulle applicazioni.	GameLift Applicazione Streams	`AWS::GameLiftStreams::Application`
Amazon GameLift Stream	Attività delle API di streaming di Amazon GameLift Streams sui gruppi di stream.	GameLift Gruppo di stream Streams	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Attività dell'API su tabelle create da Lake Formation.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	Attività dell' GuardDuty API Amazon per un rilevatore.	GuardDuty rilevatore	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging attività delle API sugli archivi dati.	MedicalImaging archivio dati	`AWS::MedicalImaging::Datastore`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass su una versione componente. **Note** Greengrass non registra gli eventi di accesso negato.	Versione componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass in una distribuzione. **Note** Greengrass non registra gli eventi di accesso negato.	Implementazione IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Attività dell' SiteWise API IoT sugli asset.	SiteWise Risorsa IoT	`AWS::IoTSiteWise::Asset`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT SiteWise	Attività dell' SiteWise API IoT su serie temporali.	Serie SiteWise temporali IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT SiteWise Assistente	Attività dell'API Sitewise Assistant sulle conversazioni.	Conversazione con Sitewise Assistant	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'entità.	TwinMaker Entità IoT	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'area di lavoro.	Spazio di TwinMaker lavoro IoT	`AWS::IoTTwinMaker::Workspace`
Classificazione intelligente di Amazon Kendra	Attività dell'API Amazon Kendra Intelligent Ranking sui piani di esecuzione di rescore.	Classificazione Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces su una tabella.	Tabella Cassandra	`AWS::Cassandra::Table`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces (per Apache Cassandra) sugli stream Cassandra CDC.	Stream Cassandra CDC	`AWS::Cassandra::Stream`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sugli stream.	Stream Kinesis	`AWS::Kinesis::Stream`
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sui consumatori di streaming.	Kinesis Stream Consumer	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Attività dell'API Kinesis Video Streams sui flussi video, ad esempio chiamate verso e. `GetMedia` `PutMedia`	Flusso video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda attività di esecuzione delle funzioni (l'API). `Invoke`	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Attività dell'API Amazon Location Maps.	Mappe geografiche	`AWS::GeoMaps::Provider`
Luoghi di Amazon Location	Attività dell'API Amazon Location Places.	Luoghi geografici	`AWS::GeoPlaces::Provider`
Route di Amazon Location	Attività dell'API Amazon Location Routes.	Percorsi geografici	`AWS::GeoRoutes::Provider`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Machine Learning	Attività dell'API di Machine Learning sui modelli ML.	Apprendimento automatico MlModel	`AWS::MachineLearning::MlModel`
Blockchain gestita da Amazon	Attività dell'API Blockchain gestita da Amazon su una rete.	Rete Blockchain gestita	`AWS::ManagedBlockchain::Network`
Blockchain gestita da Amazon	Chiamate JSON-RPC di Blockchain gestita da Amazon sui nodi Ethereum, come `eth_getBalance` o `eth_getBlockByNumber` .	Blockchain gestita	`AWS::ManagedBlockchain::Node`
Query su Blockchain gestita da Amazon	Attività dell'API Amazon Managed Blockchain Query.	Query Blockchain gestita	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	Attività dell'API Amazon MWAA negli ambienti.	Apache Airflow gestito	`AWS::MWAA::Environment`
Grafo Amazon Neptune	Attività dell'API dati, ad esempio query, algoritmi o ricerca vettoriale, su un grafo Neptune.	Grafo Neptune	`AWS::NeptuneGraph::Graph`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon One Enterprise	Attività dell'API Amazon One Enterprise su un UKey.	Amazon Uno UKey	`AWS::One::UKey`
Amazon One Enterprise	Attività dell'API Amazon One Enterprise sugli utenti.	Utente Amazon One	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sugli alias.	Alias di crittografia dei pagamenti	`AWS::PaymentCryptography::Alias`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sulle chiavi.	Chiave di crittografia dei pagamenti	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	Attività dell'API Amazon Pinpoint su applicazioni di targeting per dispositivi mobili.	Applicazione di targeting mobile	`AWS::Pinpoint::App`
App Amazon Q	Attività delle API di dati su Amazon Q Apps.	App Amazon Q	`AWS::QApps::QApp`
App Amazon Q	Attività delle API di dati nelle sessioni di Amazon Q App.	Sessione dell'app Amazon Q	`AWS::QApps::QAppSession`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Q Business	Attività dell'API Amazon Q Business su un'applicazione.	Applicazione Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Business	Attività dell'API Amazon Q Business su un'origine dati.	Origine dati Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Business	Attività dell'API Amazon Q Business su un indice.	Indice Amazon Q Business	`AWS::QBusiness::Index`
Amazon Q Business	Attività dell'API Amazon Q Business su un'esperienza Web.	Esperienza Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Attività dell'API Amazon Q Developer su un'integrazione.	Integrazione con Q Developer	`AWS::QDeveloper::Integration`
Amazon Q Developer	Attività dell'API Amazon Q Developer sulle indagini operative.	AIOps Gruppo di indagine	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	`InvokeEndpointWithResponseStream` Attività di Amazon SageMaker AI sugli endpoint.	SageMaker Endpoint AI	`AWS::SageMaker::Endpoint`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui feature store.	SageMaker AI feature store	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui componenti di prova sperimentali.	SageMaker Component e di prova dell'esperimento AI Metrics	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	Attività dell'API Signer sulla firma dei lavori.	Firmatario che firma un lavoro	`AWS::Signer::SigningJob`
AWS Signer	Attività dell'API Signer sulla firma dei profili.	Profilo di firma del firmatario	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui set di configurazione.	Set di configurazione SES	`AWS::SES::ConfigurationSet`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sulle identità e-mail.	Identità SES	`AWS::SES::EmailIdentity`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui modelli.	Modello SES	`AWS::SES::Template`
Amazon SimpleDB	Attività dell'API Amazon SimpleDB sui domini.	Dominio SimpleDB	`AWS::SDB::Domain`
AWS Step Functions	Attività dell'API Step Functions sulle attività.	Step Functions	`AWS::StepFunctions::Activity`
AWS Step Functions	Attività dell'API Step Functions su macchine a stati.	Macchina a stati di Step Functions	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	Attività dell'API Systems Manager sui canali di controllo.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	Attività dell'API Systems Manager sulle valutazioni dell'impatto.	Valutazione dell'impatto SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Attività dell'API Systems Manager sui nodi gestiti.	Nodo gestito da Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sui database.	Database Timestream	`AWS::Timestream::Database`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Timestream	Attività dell'API Amazon Timestream sugli endpoint regionali.	Endpoint regionale Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sulle tabelle.	Tabella Timestream	`AWS::Timestream::Table`
Autorizzazioni verificate da Amazon	Attività dell'API Autorizzazioni verificate da Amazon su un archivio di policy.	Autorizzazioni verificate da Amazon	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client su un dispositivo.	Dispositivo Thin client	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client in un ambiente.	Ambiente Thin client	`AWS::ThinClient::Environment`
AWS X-Ray	Attività dell'API X-Ray sulle tracce.	Traccia a raggi X	`AWS::XRay::Trace`

Quando si crea un percorso o un datastore di eventi, gli eventi di dati non vengono registrati per impostazione predefinita. Per registrare gli eventi CloudTrail relativi ai dati, è necessario aggiungere esplicitamente ogni tipo di risorsa per cui si desidera raccogliere attività. Per ulteriori informazioni sulla registrazione degli eventi di dati, consulta Registrazione degli eventi di dati.

Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per i CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Eventi relativi alle attività di rete

CloudTrail gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Gli eventi di attività di rete forniscono visibilità sulle operazioni sulle risorse eseguite all'interno di un VPC.

È possibile registrare gli eventi di attività di rete per i seguenti servizi:

- AWS AppConfig
- AWS B2B Data Interchange
- Gestione dei costi e fatturazione
- Calcolatore dei prezzi AWS
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail
- Esportazioni di dati AWS
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EventBridge Scheduler
- Piano gratuito di AWS
- Amazon FSx
- AWS IoT FleetWise
- Fatturazione AWS
- AWS KMS
- AWS Lambda
- Amazon Lookout per le apparecchiature
- Amazon Rekognition
- Amazon S3

> **Note**
>
> Gli access point multiregionali di Amazon S3 non sono supportati.

- AWS Secrets Manager
- Strumento di gestione degli incidenti AWS Systems Manager
- Amazon Textract
- Amazon WorkMail

Per impostazione predefinita, gli eventi relativi alle attività di rete non vengono registrati quando si crea un archivio dati di percorsi o eventi. Per registrare gli eventi CloudTrail di attività di rete, è necessario impostare in modo esplicito l'origine dell'evento per cui si desidera raccogliere l'attività. Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.

Si applicano costi aggiuntivi per la registrazione degli eventi di attività di rete. Per CloudTrail informazioni sui prezzi, consulta la sezione AWS CloudTrail Prezzi.

Eventi Insights

CloudTrail Gli eventi Insights rilevano attività insolite relative alla frequenza delle chiamate API o al tasso di errore nel tuo AWS account analizzando l'attività di CloudTrail gestione. Gli eventi Insights forniscono informazioni importanti, come l'API associata, codice di errore, l'ora dell'incidente e le statistiche, che ti permettono di comprendere l'attività insolita e intervenire. A differenza di altri tipi di eventi acquisiti in un archivio dati di CloudTrail trail o event, gli eventi di Insights vengono registrati solo quando CloudTrail rilevano cambiamenti nell'utilizzo dell'API dell'account o nella registrazione del tasso di errore che differiscono significativamente dai modelli di utilizzo tipici dell'account. Per ulteriori informazioni, consulta Lavorare con CloudTrail Insights.

Alcuni esempi di attività che potrebbero generare eventi Insights:

- L'account in genere registra non più di 20 chiamate API `deleteBucket` Amazon S3 al minuto, ma l'account inizia a registrare una media di 100 chiamate API `deleteBucket` al minuto. Un evento Insights viene registrato all'inizio dell'attività insolita e un altro evento Insights viene registrato per contrassegnare la fine dell'attività insolita.
- Il tuo account registra in genere 20 chiamate al minuto verso l' `EC2AuthorizeSecurityGroupIngress`API Amazon, ma inizia a registrare zero chiamate

versoAuthorizeSecurityGroupIngress. Un evento Insights viene registrato all'inizio dell'attività insolita; dieci minuti dopo, al termine dell'attività insolita, viene registrato un altro evento Insights per contrassegnare la fine dell'attività insolita.

- In genere, il tuo account registra meno di un errore AccessDeniedException in un periodo di sette giorni su API AWS Identity and Access Management , DeleteInstanceProfile. Il tuo account inizia a registrare una media di 12 errori AccessDeniedException al minuto nella chiamata API DeleteInstanceProfile. Un evento Insights viene registrato all'inizio dell'attività di tasso di errore insolita e un altro evento Insights viene registrato per contrassegnare la fine dell'attività insolita.

Questi esempi sono solo a scopo illustrativo. I risultati potrebbero variare a seconda del caso d'uso.

Per registrare gli eventi di CloudTrail Insights, devi abilitare esplicitamente gli eventi Insights su un trail o un data store di eventi nuovo o esistente. Per ulteriori informazioni sulla creazione di un trail, consulta Creazione di un percorso con la CloudTrail console. Per ulteriori informazioni sulla creazione di un datastore di eventi, consulta Crea un archivio dati sugli eventi per gli eventi Insights con la console.

Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Cronologia degli eventi

CloudTrail la cronologia degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione in un. CloudTrail Regione AWS Puoi utilizzare questa cronologia per ottenere visibilità sulle azioni intraprese nel tuo AWS account negli strumenti da riga di comando e in AWS SDKs altri servizi. AWS Management Console AWS Puoi personalizzare la visualizzazione della cronologia degli eventi nella CloudTrail console selezionando le colonne da visualizzare. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Trail

Un trail è una configurazione che consente l'invio di CloudTrail eventi a un bucket S3, con consegna opzionale a CloudWatch Logs e Amazon. EventBridge Puoi utilizzare un percorso per scegliere gli CloudTrail eventi da inviare, crittografare i file di registro degli CloudTrail eventi con una AWS KMS

chiave e configurare le notifiche di Amazon SNS per la consegna dei file di registro. Per ulteriori informazioni su come creare e gestire un trail, consulta Creare un percorso per il tuo Account AWS.

Percorsi multiregione e singola regione

Puoi creare percorsi multiregione e a regione singola per i tuoi. Account AWS

Percorsi multiregionali

Quando crei un percorso multiregionale, CloudTrail registra gli eventi in tutto ciò Regioni AWS che è abilitato nel tuo Account AWS e invia i file di registro degli CloudTrail eventi a un bucket S3 da te specificato. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multiregionali. È possibile convertire un percorso a regione singola in un percorso multiregionale utilizzando. AWS CLI Per ulteriori informazioni, consulta Comprendere i percorsi multiregionali e le regioni opt-in, Creazione di un percorso con la console e Conversione di un percorso a regione singola in un percorso multiregionale.

Percorsi a regione singola

Quando crei un percorso a regione singola, CloudTrail registra solo gli eventi in quella regione. Quindi invia i file di registro CloudTrail degli eventi a un bucket Amazon S3 specificato dall'utente. Puoi creare un percorso basato su una singola Regione solo utilizzando la AWS CLI. Se crei percorsi singoli aggiuntivi, puoi fare in modo che questi percorsi consegnino i file di registro CloudTrail degli eventi nello stesso bucket S3 o in bucket separati. Questa è l'opzione predefinita quando crei un trail utilizzando AWS CLI o l'API. CloudTrail Per ulteriori informazioni, consulta Creazione, aggiornamento e gestione di percorsi con AWS CLI.

> **Note**
>
> Per entrambi i tipi di percorsi, puoi specificare un bucket Amazon S3 di qualsiasi Regione.

Un percorso multiregionale presenta i seguenti vantaggi:

- Le impostazioni di configurazione per il percorso si applicano in modo coerente a tutti gli utenti abilitati Regioni AWS.
- Ricevi CloudTrail eventi da tutti gli utenti abilitati Regioni AWS in un singolo bucket Amazon S3 e, facoltativamente, in un CloudWatch gruppo di log Logs.

- Puoi gestire le configurazioni dei trail per tutti i dispositivi abilitati da un'unica posizione. Regioni AWS

La creazione di un percorso multiregionale ha i seguenti effetti:

- CloudTrail invia i file di log per l'attività dell'account da tutti gli account abilitati Regioni AWS al singolo bucket Amazon S3 specificato e, facoltativamente, a un CloudWatch gruppo di log Logs.
- Se hai configurato un argomento Amazon SNS per il percorso, le notifiche SNS sulle consegne di file di log in all enabled Regioni AWS vengono inviate a quel singolo argomento SNS.
- Puoi vedere il percorso multiregionale in tutte le versioni abilitate Regioni AWS, ma puoi modificare solo il percorso nella regione di origine in cui è stato creato.

Indipendentemente dal fatto che un percorso sia multiregionale o monoregionale, gli eventi inviati ad Amazon EventBridge vengono ricevuti nel bus eventi di ciascuna regione, anziché in un unico bus di eventi.

Più percorsi per regione

In presenza di gruppi di utenti diversi ma correlati tra loro, ad esempio sviluppatori, personale della sicurezza e revisori IT, puoi creare più trail per regione. Ciò consente a ciascun gruppo di ricevere la propria copia dei file di log.

CloudTrail supporta cinque percorsi per regione. Un percorso multiregionale conta come un percorso per regione.

Di seguito è riportato un esempio di regione con cinque sentieri:

- Crei due percorsi nella regione Stati Uniti occidentali (California settentrionale), ciascuno dei quali è valido solo per questa regione.
- Si creano altri due percorsi multiregione nella regione Stati Uniti occidentali (California settentrionale).
- Si crea un altro percorso multiregionale nella regione Asia Pacifico (Sydney). Questo percorso esiste anche come percorso nella regione Stati Uniti occidentali (California settentrionale).

È possibile visualizzare un elenco di percorsi Regione AWS in una pagina Percorsi della CloudTrail console. Per ulteriori informazioni, consulta Aggiornamento di un percorso con la CloudTrail console. Per CloudTrail i prezzi, consulta la sezione AWS CloudTrail Prezzi.

Percorsi organizzativi

Un percorso organizzativo è una configurazione che consente la distribuzione di CloudTrail eventi nell'account di gestione e in tutti gli account dei membri di un' AWS Organizations organizzazione nello stesso bucket Amazon S3 CloudWatch , Logs e Amazon. EventBridge La creazione di un percorso dell'organizzazione ti consente di definire una strategia di registrazione degli eventi coerente per la tua organizzazione.

Tutti gli itinerari organizzativi creati utilizzando la console sono percorsi organizzativi multiregionali che registrano gli eventi dagli account abilitati Regioni AWS in ogni account membro dell'organizzazione. Per registrare gli eventi in tutte le AWS partizioni dell'organizzazione, crea un itinerario organizzativo multiregionale in ogni partizione. È possibile creare un itinerario organizzativo a regione singola o multiarea utilizzando. AWS CLI Se si crea un itinerario a regione singola, si registra l'attività solo nel percorso Regione AWS (noto anche come regione principale).

Sebbene la Regioni AWS maggior parte sia abilitata di default per la tua Account AWS, devi abilitare manualmente alcune regioni (chiamate anche regioni opzionali). Per informazioni sulle regioni abilitate per impostazione predefinita, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Gestione dell'account AWS Guida di riferimento. Per l'elenco delle regioni CloudTrail supportate, vedere. CloudTrail Regioni supportate

Quando crei un percorso organizzativo, una copia del percorso con il nome che gli hai assegnato viene creata negli account dei membri che appartengono alla tua organizzazione.

- Se l'organigramma riguarda una singola regione e la regione di origine del percorso non è una regione che ha aderito, viene creata una copia del percorso nella regione di origine dell'organigramma in ogni account membro.
- Se l'organizzazione trail è per una regione singola e la regione di origine del percorso è una regione che ha aderito, una copia del percorso viene creata nella regione di origine dell'organizzazione negli account dei membri che hanno abilitato tale regione.
- Se il percorso organizzativo è multiregionale e la regione di origine del percorso non è una regione che accetta l'iscrizione, viene creata una copia del percorso in ogni account membro abilitato Regione AWS . Quando un account membro abilita una regione con iscrizione, una volta completata l'attivazione di tale regione, viene creata una copia del percorso multiregionale nella regione appena attivata per l'account membro.
- Se il percorso organizzativo è multiregionale e la regione di origine è una regione con attivazione, gli account dei membri non invieranno attività al percorso organizzativo a meno che non scelgano il luogo in Regione AWS cui è stato creato il percorso multiregionale. Ad esempio, se crei un

percorso multiregionale e scegli la regione Europa (Spagna) come regione di origine del percorso, solo gli account dei membri che hanno abilitato la regione Europa (Spagna) per il proprio account invieranno l'attività dell'account all'organigramma.

> **Note**
>
> CloudTrail crea gli itinerari organizzativi negli account dei membri anche se la convalida di una risorsa fallisce. Alcuni esempi di errori di convalida includono:
>
> - una policy sui bucket Amazon S3 errata
> - una politica tematica di Amazon SNS errata
> - impossibilità di effettuare consegne a un gruppo di CloudWatch log di Logs
> - autorizzazione insufficiente per crittografare utilizzando una chiave KMS
>
> Un account membro con CloudTrail autorizzazioni può visualizzare eventuali errori di convalida di un percorso organizzativo visualizzando la pagina dei dettagli del percorso sulla CloudTrail console o eseguendo il comando. AWS CLI get-trail-status

Gli utenti con CloudTrail autorizzazioni negli account dei membri saranno in grado di visualizzare gli itinerari dell'organizzazione (incluso l'ARN del percorso) quando accedono CloudTrail alla console dai AWS propri account o quando AWS CLI eseguono comandi `describe-trails` come (sebbene gli account membro debbano utilizzare l'ARN per l'itinerario dell'organizzazione e non il nome, quando utilizzano il). AWS CLI Tuttavia, gli utenti degli account membro non disporranno delle autorizzazioni sufficienti per eliminare gli itinerari organizzativi, attivare o disattivare la connessione, modificare i tipi di eventi registrati o modificare in altro modo gli itinerari organizzativi. Per ulteriori informazioni su AWS Organizations, consulta Concetti e terminologia di Organizations. Per ulteriori informazioni sulla creazione e sull'utilizzo di trail dell'organizzazione, consulta Creazione di un percorso per un'organizzazione.

CloudTrail Archivi di dati su laghi ed eventi

CloudTrail Lake ti consente di eseguire query granulari basate su SQL sui tuoi eventi e di registrare gli eventi da fonti esterne AWS, incluse le tue applicazioni, e dai partner che sono integrati con. CloudTrail Non è necessario che nel tuo account sia configurato un percorso per usare Lake. CloudTrail

Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili in base ai criteri selezionati applicando i selettori di eventi avanzati. Puoi conservare i dati degli eventi in un datastore di eventi per un massimo di 3.653 giorni (circa 10 anni) se scegli l'opzione Prezzo per la conservazione estendibile di un anno o di 2.557 giorni (circa 7 anni) se scegli l'opzione Prezzo per la conservazione di sette anni. Puoi salvare le query Lake per l'utilizzo futuro e visualizzarne i risultati per un massimo di sette giorni. Puoi anche salvare i risultati delle query in un bucket S3. CloudTrail Lake può anche archiviare eventi di un'organizzazione AWS Organizations in un data store di eventi o eventi provenienti da più regioni e account. CloudTrail Lake fa parte di una soluzione di controllo che consente di eseguire indagini di sicurezza e risoluzione dei problemi. Per ulteriori informazioni, consultare Lavorare con AWS CloudTrail Lake e CloudTrail Concetti e terminologia dei laghi.

CloudTrail Approfondimenti

CloudTrail Gli approfondimenti aiutano AWS gli utenti a identificare e rispondere a volumi insoliti di chiamate API o errori registrati nelle chiamate API analizzando continuamente gli eventi di CloudTrail gestione. Un evento Insights è un registro di livelli insoliti di attività API di gestione `write` o livelli insoliti di errori restituiti nell'attività dell'API di gestione. Per impostazione predefinita, i percorsi e gli archivi dati degli eventi non registrano gli eventi di CloudTrail Insights. Nella console puoi scegliere di registrare gli eventi Insights quando crei o aggiorni un percorso o un datastore di eventi. Quando utilizzi l' CloudTrail API, puoi registrare gli eventi di Insights modificando le impostazioni di un trail o di un data store di eventi esistente con l'`PutInsightSelectors`API. Si applicano costi aggiuntivi per la registrazione degli eventi di CloudTrail Insights. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consulta Lavorare con CloudTrail Insights e Prezzi di AWS CloudTrail.

Tag

Un tag è una chiave definita dal cliente e un valore opzionale che può essere assegnato a AWS risorse come CloudTrail percorsi, archivi di dati di eventi e canali, bucket S3 utilizzati per archiviare file di CloudTrail registro, AWS Organizations organizzazioni e unità organizzative e molto altro. Aggiungendo gli stessi tag ai percorsi e ai bucket S3 utilizzati per archiviare i file di registro dei percorsi, puoi semplificare la gestione, la ricerca e il filtraggio di queste risorse. AWS Resource Groups È possibile implementare strategie di utilizzo dei tag per aiutarti in maniera regolare, efficace e semplice a trovare e gestire le risorse. Per ulteriori informazioni, consulta Best Practices for AWS Tagging Resources.

AWS Security Token Service e CloudTrail

AWS Security Token Service (AWS STS) è un servizio che dispone di un endpoint globale e supporta anche endpoint specifici della regione. Un endpoint è un URL che rappresenta il punto di partenza per le richieste di un servizio Web. Ad esempio, `https://cloudtrail.us-west-2.amazonaws.com` è il punto di ingresso regionale del servizio negli Stati Uniti occidentali (Oregon). AWS CloudTrail Gli endpoint regionali consentono di ridurre la latenza nelle applicazioni.

Quando si utilizza un endpoint AWS STS specifico di una regione, il percorso in quella regione riporta solo gli AWS STS eventi che si verificano in quella regione. Ad esempio, se utilizzi l'endpoint `sts.us-west-2.amazonaws.com`, il trail nella regione us-west-2 distribuisce solo gli eventi AWS STS che hanno origine nella regione us-west-2. Per ulteriori informazioni sugli endpoint AWS STS regionali, consulta Attivazione e disattivazione AWS STS in una AWS regione nella Guida per l'utente IAM.

Per un elenco completo degli endpoint AWS regionali, consulta AWS Regioni ed endpoint nel. Riferimenti generali di AWS Per ulteriori informazioni sugli eventi che hanno origine dall'endpoint AWS STS globale, consulta Eventi dei servizi globali.

Eventi dei servizi globali

> **Important**
>
> A partire dal 22 novembre 2021, è AWS CloudTrail cambiato il modo in cui i trail registrano gli eventi di servizio globale. Ora, gli eventi creati da Amazon CloudFront AWS STS vengono registrati nella regione in cui sono stati creati, la regione Stati Uniti orientali (Virginia settentrionale), us-east-1. AWS Identity and Access Management In questo modo il modo in cui vengono CloudTrail trattati questi servizi è coerente con quello di altri servizi globali. AWS Per continuare a ricevere eventi di assistenza globale al di fuori della regione Stati Uniti orientali (Virginia settentrionale), assicurati di convertire i percorsi a Regione singola che utilizzano eventi di assistenza globale al di fuori di Stati Uniti orientali (Virginia settentrionale) in percorsi multi-regione. Per ulteriori informazioni sull'acquisizione di eventi di assistenza globale, consulta Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale più avanti in questa sezione.
> Al contrario, la cronologia degli eventi nella CloudTrail console e il aws cloudtrail lookup-events comando mostreranno questi eventi nel luogo in Regione AWS cui si sono verificati.

Per la maggior parte dei servizi, gli eventi vengono registrati nella regione in cui si è verificata l'operazione. Per i servizi globali come AWS Identity and Access Management (IAM) e Amazon AWS STS CloudFront, gli eventi vengono distribuiti su qualsiasi percorso che includa servizi globali.

Per la maggior parte dei servizi globali, gli eventi sono registrati come se si verificassero nella Regione Stati Uniti orientali (Virginia settentrionale), ma alcuni eventi dei servizi globali sono registrati come se si verificassero in altre Regioni, come Stati Uniti orientali (Ohio) o Stati Uniti occidentali (Oregon).

Per evitare la ricezione di eventi di servizi globali duplicati, considerare quanto segue:

- Gli eventi di servizio globali vengono forniti per impostazione predefinita ai percorsi creati utilizzando la CloudTrail console. Gli eventi vengono distribuiti nel bucket associato al trail.
- In presenza di più percorsi validi per una singola Regione, valuta l'ipotesi di configurare i percorsi in modo che gli eventi di servizi globali vengano distribuiti solo in uno dei percorsi. Per ulteriori informazioni, consulta Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale.
- Se si converte un itinerario multiregionale in un percorso a regione singola, la registrazione degli eventi del servizio globale viene disattivata automaticamente per quel percorso. Analogamente, se si converte un itinerario a regione singola in un percorso multiregionale, la registrazione degli eventi del servizio globale viene attivata automaticamente per quel percorso.

  Per ulteriori informazioni sulla modifica della registrazione degli eventi dei servizi globali per un trail, consulta Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale.

Esempio:

1. È possibile creare un percorso nella console. CloudTrail Per impostazione di default, questo trail registra gli eventi dei servizi globali.
2. Disponi di più percorsi validi per una singola Regione.
3. Non è necessario includere i servizi globali per i percorsi di una singola Regione. Gli eventi dei servizi globali vengono distribuiti al primo trail. Per ulteriori informazioni, consulta Creazione, aggiornamento e gestione di percorsi con AWS CLI.

> **Note**
>
> Quando crei o aggiorni un itinerario con AWS CLI AWS SDKs, o CloudTrail API, puoi specificare se includere o escludere gli eventi di servizio globale per i percorsi. Non è possibile configurare la registrazione degli eventi del servizio globale dalla CloudTrail console.

CloudTrail Regioni supportate

> **Note**
>
> Per informazioni sulle regioni supportate da CloudTrail Lake, consultaCloudTrail Regioni supportate dai laghi.
> Per informazioni sugli endpoint del piano dati, vedere Endpoint del piano dati in. Riferimenti generali di AWS

Nome Regione	Regione	Endpoint del piano di controllo	Protocollo	Data di supporto
US East (N. Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	13/11/2013
Stati Uniti orientali (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	17/10/2016
US West (N. California)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	13/05/2014
US West (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	13/11/2013
Africa (Cape Town)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	22/04/2020

Nome Regione	Regione	Endpoint del piano di controllo	Protocollo	Data di supporto
Asia Pacifico (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	04/24/2019
Asia Pacific (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	22/11/2022
Asia Pacifico (Giacarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	13/12/2021
Asia Pacifico (Malesia)	ap-southeast-5	cloudtrail.ap-southeast-5.amazonaws.com	HTTPS	22/08/2024
Asia Pacifico (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	23/01/2023
Asia Pacific (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	27/06/2016
Asia Pacifico (Osaka-Locale)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	12/02/2018
Asia Pacifico (Seul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	06/01/2016
Asia Pacific (Singapore)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	06/30/2014

Nome Regione	Regione	Endpoint del piano di controllo	Protocollo	Data di supporto
Asia Pacific (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	13/05/2014
Asia Pacifico (Tailandia)	ap-southeast-7	cloudtrail.ap-southeast-7.amazonaws.com	HTTPS	01/07/2025
Asia Pacifico (Tokyo)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	06/30/2014
Canada (Central)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	08/12/2016
Canada occidentale (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	20/12/2023
China (Beijing)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	03/01/2014
Cina (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	11/12/2017
Europe (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	23/10/2014
Europa (Irlanda)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	13/05/2014
Europe (London)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	13/12/2016
Europa (Milano)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	27/04/2020

Nome Regione	Regione	Endpoint del piano di controllo	Protocollo	Data di supporto
Europe (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	18/12/2017
Europa (Spagna)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	16/11/2022
Europa (Stoccolma)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	11/12/2018
Europa (Zurigo)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Israele (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	31/07/2023
Messico (centrale)	mx-central-1	cloudtrail.mx-central-1.amazonaws.com	HTTPS	13/01/2025
Medio Oriente (Bahrein)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	29/07/2019
Medio Oriente (Emirati Arabi Uniti)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	30/08/2022
Sud America (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	06/30/2014
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	11/12/2018

Nome Regione	Regione	Endpoint del piano di controllo	Protocollo	Data di supporto
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	08/16/2011

Per ulteriori informazioni sull'utilizzo CloudTrail in AWS GovCloud (US) Regions, consulta Service Endpoints nella Guida per l'AWS GovCloud (US) utente.

Per ulteriori informazioni sull'utilizzo CloudTrail nella regione Cina (Pechino), consulta Endpoints e ARNs per AWS in Cina nella Riferimenti generali di Amazon Web Services.

CloudTrail servizi e integrazioni supportati

CloudTrail supporta la registrazione degli eventi per molti. Servizi AWS Puoi trovare le specifiche per ciascun servizio supportato nella guida del servizio in questione. Per un elenco di argomenti specifici del servizio, vedere. AWS argomenti di servizio per CloudTrail Inoltre, alcuni Servizi AWS possono essere utilizzati per analizzare e agire in base ai dati raccolti nei CloudTrail log.

> **Note**
>
> Per un elenco delle Regioni supportate da ciascun servizio, consulta Endpoint e quote del servizio nella Riferimenti generali di Amazon Web Services.

Argomenti

- AWS integrazioni di servizi con registri CloudTrail
- CloudTrail integrazione con Amazon EventBridge
- CloudTrail integrazione con AWS Organizations
- CloudTrail integrazione con AWS Control Tower
- CloudTrail integrazione con Amazon Security Lake
- CloudTrail Integrazione di Lake con Amazon Athena
- CloudTrail Integrazione di Lake con AWS Config

- CloudTrail Integrazione lacustre con AWS Audit Manager
- AWS argomenti di servizio per CloudTrail
- CloudTrail servizi non supportati

AWS integrazioni di servizi con registri CloudTrail

> **Note**
>
> Puoi anche usare CloudTrail Lake per interrogare e analizzare i tuoi eventi. CloudTrail Le query su Lake offrono una visione più approfondita e personalizzabile degli eventi rispetto alle semplici ricerche di chiavi e valori nella cronologia degli eventi o in corso. `LookupEvents` CloudTrail Gli utenti di Lake possono eseguire query SQL (Standard Query Language) complesse su più campi di un evento. CloudTrail Per ulteriori informazioni, consultare Lavorare con AWS CloudTrail Lake e Copiare gli eventi del percorso su CloudTrail Lake. CloudTrail Gli archivi di dati e le richieste di Lake Event sono a pagamento. CloudTrail Per ulteriori informazioni sui prezzi di CloudTrail Lake, consulta la sezione Prezzi.AWS CloudTrail

Puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta i seguenti argomenti.

AWS Servizio	Argomento	Descrizione
Amazon Athena	Interrogazione dei registri AWS CloudTrail	L'utilizzo di Athena con CloudTrail i log è un modo efficace per migliorare l'analisi dell'attività di AWS servizio. Ad esempio, puoi utilizzar e le query per identificare le tendenze e isolare con maggiore precisione le attività in base a un attributo specifico , ad esempio l'indirizzo IP di origine o un utente.

AWS Servizio	Argomento	Descrizione
		Puoi creare automaticamente tabelle per interrogare i log direttamente dalla CloudTrai l console e utilizzarle per eseguire query in Athena. Per ulteriori informazioni, consulta Creare una tabella per CloudTrail i log nella CloudTrail console nella Guida per l'utente di Amazon Athena. **Note** L'esecuzione di query in Amazon Athena comporta costi supplementari. Per ulteriori informazioni, consulta Prezzi di Amazon Athena.

AWS Servizio	Argomento	Descrizione
CloudWatch Registri Amazon	Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs	Puoi configurare CloudTrai l con CloudWatch Logs per monitorare i tuoi trail log e ricevere notifiche quando si verificano attività specifiche. Ad esempio, puoi definire filtri metrici CloudWatch Logs che attiveranno gli CloudWatch allarmi e ti invieranno notifiche quando tali allarmi vengono attivati. **Note** Si applicano i prezzi standard per Amazon CloudWatch e Amazon CloudWatc h Logs. Per ulteriori informazioni, consulta Prezzi di Amazon CloudWatch .

CloudTrail integrazione con Amazon EventBridge

Amazon EventBridge è un AWS servizio che fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle AWS risorse. In EventBridge, puoi creare regole che rispondono agli eventi registrati da CloudTrail. Per ulteriori informazioni, consulta Creare una regola in Amazon EventBridge.

Puoi offrire eventi a cui sei abbonato durante il periodo di validità della registrazione EventBridge creando una regola con la EventBridge console.

Dalla EventBridge console:

- Scegli il `AWS API Call via CloudTrail` tipo di dettaglio per fornire CloudTrail dati ed eventi di gestione con un `eventType` di. `AwsApiCall` Per registrare eventi con un valore di tipo dettaglio pari a`AWS API Call via CloudTrail`, è necessario disporre di un percorso che attualmente registri gli eventi di gestione o relativi ai dati.
- Scegli il `AWS Console Sign In via CloudTrail` tipo di dettaglio per fornire gli eventi di accesso.AWS Management Console Per registrare eventi con un tipo di dettaglio di`AWS Console Sign In via CloudTrail`, è necessario disporre di un percorso che attualmente registri gli eventi di gestione.
- Scegli il `AWS Insight via CloudTrail` tipo di dettaglio per fornire gli eventi Insights. Per registrare eventi con un valore di tipo dettaglio pari a`AWS Insight via CloudTrail`, è necessario disporre di un percorso che attualmente registri gli eventi di Insights. Per ulteriori informazioni sulla registrazione di eventi Insights, consulta Lavorare con CloudTrail Insights.

Per informazioni su come creare e un percorso, consulta Creazione di un percorso con la CloudTrail console.

CloudTrail integrazione con AWS Organizations

L'account di gestione di un' AWS Organizations organizzazione può aggiungere un amministratore delegato per gestire le CloudTrail risorse dell'organizzazione. Puoi creare un percorso o un datastore di eventi dell'organizzazione nell'account di gestione o nell'account dell'amministratore delegato per un'organizzazione che raccoglie tutti i dati degli eventi per tutti gli account AWS di un'organizzazione in AWS Organizations. La creazione di un percorso organizzativo o di un archivio dati di eventi organizzativi consente di definire una strategia di registrazione degli eventi uniforme per l'organizzazione.

CloudTrail integrazione con AWS Control Tower

AWS Control Tower imposta una nuova CloudTrail organizzazione per la gestione del trail logging degli eventi quando si configura una landing zone. Quando si registra un account AWS Control Tower, quest'ultimo è regolato dall'organigramma dell'organizzazione dell'organizzazione. AWS Control Tower Se disponi di un percorso organizzativo esistente in quell'account, potresti visualizzare addebiti duplicati, a meno che non elimini l'itinerario esistente per l'account prima di registrarlo. AWS Control Tower Puoi visualizzare la pagina Percorsi sulla CloudTrail console per vedere se sono stati creati degli itinerari organizzativi. Per ulteriori informazioni in merito AWS Control Tower, consulta Informazioni sull'accesso AWS Control Tower nella Guida per l'AWS CloudTrail utente.

CloudTrail integrazione con Amazon Security Lake

Security Lake può raccogliere i log associati agli eventi di CloudTrail gestione e agli eventi relativi ai CloudTrail dati per S3 e Lambda. Per ulteriori informazioni, consulta i registri CloudTrail degli eventi nella Guida per l'utente di Amazon Security Lake.

Per raccogliere eventi di CloudTrail gestione in Security Lake, è necessario disporre di almeno un percorso organizzativo CloudTrail multiregionale che raccolga gli eventi di gestione di lettura e scrittura CloudTrail .

CloudTrail Integrazione di Lake con Amazon Athena

Puoi eseguire la federazione di un datastore di eventi per visualizzare i metadati associati al datastore nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi utilizzando Amazon Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

CloudTrail Integrazione di Lake con AWS Config

Puoi creare un datastore di eventi per includere gli elementi di configurazione AWS Config e utilizzarlo per esaminare le modifiche non conformi agli ambienti di produzione. Per ulteriori informazioni, consulta Crea un archivio dati di eventi per gli elementi di configurazione con la console.

CloudTrail Integrazione lacustre con AWS Audit Manager

È possibile creare un archivio dati di eventi per AWS Audit Manager le prove utilizzando la console Audit Manager. Per ulteriori informazioni sull'aggregazione delle prove in CloudTrail Lake utilizzando Audit Manager, consulta Comprendere come funziona Evidence Finder con CloudTrail Lake nella Guida per l'AWS Audit Manager utente.

AWS argomenti di servizio per CloudTrail

È possibile ottenere ulteriori informazioni su come gli eventi per AWS i singoli servizi vengono registrati nei CloudTrail registri, inclusi gli eventi di esempio per quel servizio nei file di registro. Per ulteriori informazioni sull'integrazione di AWS servizi specifici CloudTrail, consulta l'argomento sull'integrazione nella guida individuale del servizio.

I servizi ancora in anteprima, non ancora rilasciati per la disponibilità generale (GA) o che non sono disponibili al pubblico APIs, non sono considerati supportati.

> **Note**
>
> Per un elenco delle Regioni supportate da ciascun servizio, consulta Endpoint e quote del servizio nella Riferimenti generali di Amazon Web Services.
> Per informazioni sui servizi che registrano gli eventi di dati, consultare Eventi di dati.

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon API Gateway	Registra le chiamate di gestione delle API su Amazon API Gateway utilizzando AWS CloudTrail	09/07/2015
Amazon AppFlow	Registrazione delle chiamate AppFlow API Amazon con AWS CloudTrail	22/04/2020
Amazon AppStream 2.0	Registrazione delle chiamate API Amazon AppStream 2.0 con AWS CloudTrail	04/25/2019
Amazon Athena	Registrazione delle chiamate API Amazon Athena con AWS CloudTrail	19/05/2017
Amazon Aurora	Monitoraggio delle chiamate API Amazon Aurora in AWS CloudTrail	31/08/2018
Amazon Bedrock	Registra le chiamate API Amazon Bedrock utilizzando AWS CloudTrail	23/10/2023
Amazon Braket	Registrazione dell'API Amazon Braket con CloudTrail	08/12/2020

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Chime	Registra le chiamate di amministrazione di Amazon Chime utilizzando AWS CloudTrail	27/09/2017
Directory del cloud Amazon	Registrazione delle chiamate API Cloud Directory utilizzan do AWS CloudTrail	26/01/2017
Amazon CloudFront	Utilizzo AWS CloudTrail per acquisire le richieste inviate all' CloudFront API	28/05/2014
Amazon CloudSearch	Registrazione delle chiamate di Amazon CloudSearch Configuration Service utilizzan do AWS CloudTrail	16/10/2014
Amazon CloudWatch	Registrazione delle chiamate CloudWatch API Amazon AWS CloudTrail	30/04/2014
CloudWatch Registri Amazon	Registrazione delle chiamate API Amazon CloudWatch Logs AWS CloudTrail	10/03/2016
Amazon CodeCatalyst	Registrazione delle chiamate CodeCatalyst API in modalità connessa tramite Account AWSAWS CloudTrail	12/01/2022
CodeGuru Revisore Amazon	Registrazione delle chiamate API Amazon CodeGuru Reviewer con AWS CloudTrail	02/12/2019

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Cognito	Registrazione delle chiamate API Amazon Cognito con AWS CloudTrail	18/02/2016
Amazon Comprehend	Registrazione delle chiamate API Amazon Comprehend con AWS CloudTrail	17/01/2018
Amazon Comprehend Medical	Registrazione delle chiamate API di Amazon Comprehen d Medical tramite AWS CloudTrail	27/11/2018
Amazon Connect	Registrazione delle chiamate API di Amazon Connect con AWS CloudTrail	11/12/2019
Amazon Data Firehose	Monitoraggio delle chiamate API Amazon Data Firehose con AWS CloudTrail	17/03/2016
Amazon Data Lifecycle Manager	Registrazione delle chiamate API di Amazon Data Lifecycle Manager tramite AWS CloudTrail	24/07/2018
Amazon Detective	Registrazione delle chiamate API di Amazon Detective con AWS CloudTrail	31/03/2020
Amazon DevOps Guru	Registrazione delle chiamate API Amazon DevOps Guru con AWS CloudTrail	05/04/2021
Amazon DocumentDB (compatibile con MongoDB)	Registrazione delle chiamate API di Amazon DocumentDB con AWS CloudTrail	01/09/2019

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon DynamoDB	Registrazione delle operazioni DynamoDB mediante AWS CloudTrail	28/05/2015
Amazon EC2	Registra le chiamate EC2 API Amazon utilizzando AWS CloudTrail	13/11/2013
Amazon EC2 Auto Scaling	Registrazione delle chiamate API Auto Scaling mediante CloudTrail	16/07/2014
Blocchi EC2 di capacità Amazon	La registrazione di Capacity Blocks le chiamate API con AWS CloudTrail	31/10/2023
Amazon EC2 Image Builder	Registrazione delle chiamate all' EC2 API Image Builder utilizzando CloudTrail	02/12/2019
Amazon Elastic Block Store (Amazon EBS) EBS diretto APIs	Registrazione delle chiamate API utilizzando AWS CloudTrail Registra le chiamate API per EBS direttamente con APIs AWS CloudTrail	Amazon EBS: 13/11/2013 EBS diretto: 30/06/2020 APIs
Amazon Elastic Container Registry (Amazon ECR)	Registrazione delle chiamate API Amazon ECR mediante AWS CloudTrail	21/12/2015
Amazon Elastic Container Service (Amazon ECS)	Registrazione delle chiamate API Amazon ECS tramite AWS CloudTrail	09/04/2015

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Elastic File System (Amazon EFS)	Registrazione delle chiamate API Amazon EFS con AWS CloudTrail	28/06/2016
Amazon Elastic Kubernetes Service (Amazon EKS)	Registrazione delle chiamate API Amazon EKS con AWS CloudTrail	06/05/2018
Amazon Elastic Transcoder	Registrazione delle chiamate API Amazon Elastic Transcoder con AWS CloudTrail	27/10/2014
Amazon ElastiCache	Registrazione delle chiamate ElastiCache API Amazon tramite AWS CloudTrail	15/09/2014
Amazon EMR	Registrazione delle chiamate API Amazon EMR utilizzando AWS CloudTrail	04/04/2014
Amazon EMR su EKS	Registrazione delle chiamate API di Amazon EMR su EKS utilizzando AWS CloudTrail	09/12/2020
Amazon EventBridge	Registrazione delle chiamate EventBridge API Amazon tramite AWS CloudTrail	11/07/2019
Amazon FinSpace	Interrogazione dei registri AWS CloudTrail	18/10/2022
Amazon Forecast	Registrazione delle chiamate API Amazon Forecast con AWS CloudTrail	28/11/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Fraud Detector	Registrazione delle chiamate API di Amazon Fraud Detector con AWS CloudTrail	01/09/2020
Amazon FSx per Lustre	Registrazione delle chiamate API Amazon FSx for Lustre con AWS CloudTrail	11/01/2019
File server Amazon FSx per Windows	Monitoraggio con AWS CloudTrail	28/11/2018
GameLift Server Amazon	Registrazione delle chiamate API di Amazon GameLift Servers con AWS CloudTrail	27/01/2016
Amazon GameLift Stream	Registrazione delle chiamate API Amazon GameLift Streams tramite AWS CloudTrail	03/05/2025
Amazon GuardDuty	Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail	12/02/2018
Amazon Inspector	Registrazione delle chiamate API Amazon Inspector tramite AWS CloudTrail	29/11/2021
Amazon Inspector Classic	Registrazione delle chiamate API Amazon Inspector Classic con AWS CloudTrail	20/04/2016
Scansione Amazon Inspector	Amazon Inspector Scansiona le informazioni in CloudTrail	27/11/2023

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Interactive Video Service	Registrazione delle chiamate API di Amazon IVS con AWS CloudTrail	15/07/2020
Amazon Kendra	Registrazione delle chiamate all'API Amazon Kendra e registrazione delle AWS CloudTrail chiamate all'API Amazon Kendra Intelligent Ranking con log AWS CloudTrail	11/05/2020
Amazon Keyspaces (per Apache Cassandra)	Registrazione delle chiamate API di Amazon Keyspaces con AWS CloudTrail	13/01/2020
Servizio gestito da Amazon per Apache Flink	Registrazione delle chiamate del servizio gestito per l'API Apache Flink con AWS CloudTrail	03/22/2019
Flusso di dati Amazon Kinesis	Registrazione delle chiamate all'API Amazon Kinesis Data Streams tramite AWS CloudTrail	25/04/2014
Amazon Kinesis Video Streams	Registrazione delle chiamate all'API Kinesis Video Streams con AWS CloudTrail	24/05/2018
Amazon Lex	Registrazione delle chiamate API Amazon Lex con CloudTrail	15/08/2017

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Lightsail	Registrazione delle chiamate API Lightsail con AWS CloudTrail	23/12/2016
Servizio di posizione Amazon	Registrazione e monitoraggio con AWS CloudTrail	15/12/2020
Amazon Lookout per le apparecchiature	Monitoraggio di Amazon Lookout for Equipment	12/01/2020
Amazon Lookout per le metriche	Visualizzazione dell'attività dell'API Amazon Lookout for Metrics in AWS CloudTrail	08/12/2020
Amazon Lookout per Vision	Registrazione delle chiamate di Amazon Lookout for Vision con AWS CloudTrail	12/01/2020
Amazon Machine Learning	Registrazione delle chiamate API Amazon ML mediante AWS CloudTrail	10/12/2015
Amazon Macie	Registrazione delle chiamate API di Amazon Macie tramite AWS CloudTrail	13/05/2020
Blockchain gestita da Amazon	Registrazione delle chiamate API di Blockchain gestita da Amazon tramite AWS CloudTrail Registrazione di Ethereum per le chiamate API di Managed Blockchain utilizzando AWS CloudTrail (anteprima)	04/01/2019

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Grafana gestito da Amazon	Registrazione delle chiamate API di Amazon Managed Grafana tramite AWS CloudTrail	15/12/2020
Amazon Managed Service per Prometheus	Registrazione delle chiamate API di Amazon Managed Service for Prometheus tramite AWS CloudTrail	15/12/2020
Amazon Managed Streaming per Apache Kafka	Registrazione delle chiamate API con AWS CloudTrail	11/12/2018
Amazon Managed Workflows for Apache Airflow	Visualizzazione dei registri di controllo AWS CloudTrail	24/11/2020
Amazon MemoryDB	Registrazione delle chiamate API Amazon MemoryDB con AWS CloudTrail	19/08/2021
Amazon MQ	Registrazione delle chiamate API Amazon MQ utilizzando AWS CloudTrail	19/07/2018
Amazon Neptune	Registrazione delle chiamate API Amazon Neptune utilizzando AWS CloudTrail	30/05/2018
Amazon One Enterprise	Registrazione delle chiamate API Amazon One Enterprise tramite AWS CloudTrail	27/11/2023
OpenSearch Servizio Amazon	Monitoraggio delle chiamate API di Amazon OpenSearch Service con AWS CloudTrail	01/10/2015

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Personalize	Registrazione delle chiamate API di Amazon Personalize con AWS CloudTrail	28/11/2018
Amazon Pinpoint	Registrazione delle chiamate API Amazon Pinpoint con AWS CloudTrail	06/02/2018
API SMS e Voce di Amazon Pinpoint	Registrazione delle chiamate API Amazon Pinpoint con AWS CloudTrail	16/11/2018
Amazon Polly	Registrazione delle chiamate API Amazon Polly con AWS CloudTrail	30/11/2016
Amazon Q Business	Registrazione delle chiamate API Amazon Q Business tramite AWS CloudTrail	28/11/2023
Amazon Q Developer	Registrazione delle chiamate API Amazon Q Developer tramite AWS CloudTrail	28/11/2023
Database Amazon Quantum Ledger (Amazon QLDB)	Registrazione delle chiamate API di Amazon QLDB con AWS CloudTrail	10/09/2019
Amazon QuickSight	Operazioni di registrazione con CloudTrail	28/04/2017
Amazon Relational Database Service (Amazon RDS)	Registrazione delle chiamate API Amazon RDS tramite AWS CloudTrail	13/11/2013

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Approfondimenti sulle prestazioni di Amazon RDS	Registrazione delle chiamate API Amazon RDS tramite AWS CloudTrail L'API Performance Insights di Amazon RDS è un subset dell'API Amazon RDS.	06/21/2018
Amazon Redshift	Registrazione delle chiamate API Amazon Redshift con AWS CloudTrail	10/06/2014
Amazon Rekognition	Registrazione delle chiamate API Amazon Rekognition utilizzando AWS CloudTrail	06/04/2018
Amazon Route 53	Utilizzo di AWS CloudTrail per acquisire le richieste inviate all'API di Route 53	11/02/2015
Amazon Application Recovery Controller (ARC)	Registrazione delle chiamate API Amazon Application Recovery Controller (ARC) utilizzando AWS CloudTrail	27/07/2021
Amazon S3	Registrazione delle chiamate API Amazon S3 tramite AWS CloudTrail	Eventi di gestione: 01/09/2015 Eventi di dati: 21/11/2016
Amazon S3 Glacier	Registrazione delle chiamate API S3 Glacier utilizzando AWS CloudTrail	11/12/2014
Amazon SageMaker AI	Registrazione delle chiamate API Amazon SageMaker AI con AWS CloudTrail	11/01/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon Security Lake	Registrazione delle chiamate API di Amazon Security Lake tramite CloudTrail	30/05/2023
Amazon Simple Email Service (Amazon SES)	Registrazione delle chiamate API Amazon SES tramite AWS CloudTrail	07/05/2015
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	Registrazione delle chiamate API Amazon SNS utilizzando AWS CloudTrail	09/10/2014
Amazon Simple Queue Service (Amazon SQS)	Registrazione delle azioni dell'API Amazon SQS tramite AWS CloudTrail	16/07/2014
Amazon Simple Workflow Service (Amazon SWF)	Registrazione delle chiamate API con AWS CloudTrail	Eventi gestionali: 13/05/2014 Data eventi: 14/02/2024
Amazon Textract	Registrazione delle chiamate API Amazon Textract con AWS CloudTrail	05/29/2019
Amazon Timestream	Registrazione delle chiamate API Timestream con AWS CloudTrail	30/09/2020
Amazon Transcribe	Registrazione delle chiamate API Amazon Transcribe con AWS CloudTrail	28/06/2018
Amazon Translate	Registrazione delle chiamate API di Amazon Translate con AWS CloudTrail	04/04/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Autorizzazioni verificate da Amazon	Registrazione delle chiamate API Amazon Verified Permissions utilizzando AWS CloudTrail	13/06/2023
Amazon Virtual Private Cloud (Amazon VPC) (Amazon VPC)	Registrazione delle chiamate API utilizzando AWS CloudTrail L'API Amazon VPC è un sottoinsieme dell'API Amazon. EC2	13/11/2013
Amazon VPC Lattice	CloudTrail logs	31/03/2023
Sistema di analisi della reperibilità Amazon VPC	Registrazione delle chiamate API Reachability Analyzer utilizzando AWS CloudTrail	27/11/2023
Amazon WorkDocs	Registrazione delle chiamate WorkDocs API Amazon tramite AWS CloudTrail	27/08/2014
Amazon WorkMail	Registrazione delle chiamate WorkMail API Amazon tramite AWS CloudTrail	12/12/2017
Amazon WorkSpaces	Registrazione delle chiamate WorkSpaces API Amazon tramite CloudTrail	09/04/2015
Amazon WorkSpaces Thin Client	Registrazione delle chiamate API Amazon WorkSpaces Thin Client utilizzando AWS CloudTrail	26/11/2023

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Amazon WorkSpaces Web	Registrazione delle chiamate Amazon WorkSpaces Web API tramite AWS CloudTrail	30/11/2021
Application Auto Scaling	Registrazione delle chiamate API Application Auto Scaling con AWS CloudTrail	31/10/2016
Gestione dell'account AWS	Registrazione delle chiamate API utilizzando Gestione dell'account AWSAWS CloudTrail	01/10/2021
AWS Amplify	Registrazione delle chiamate API di Amplify tramite AWS CloudTrail	30/11/2020
AWS App Mesh	Registrazione delle chiamate API di App Mesh con AWS CloudTrail	AWS App Mesh 30/10/2019 App Mesh Envoy Management Service 18/03/2022
AWS App Runner	Registrazione delle chiamate API App Runner con AWS CloudTrail	18/05/2021
AWS AppConfig	Registrazione AWS AppConfig delle chiamate API utilizzando AWS CloudTrail	Eventi gestionali: 31/07/2020 Data eventi: 01/04/2024
AWS AppFabric	Registrazione AWS AppFabric delle chiamate API utilizzando AWS CloudTrail	27/06/2023
AWS Application Discovery Service	Registrazione delle chiamate API di Application Discovery Service con AWS CloudTrail	12/05/2016

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Servizio di trasformazione delle applicazioni	(Servizio di backend utilizzato da AWS strumenti come AWS Microservice Extractor for .NET)	26/08/2023
AWS AppSync	Registrazione AWS AppSync delle chiamate API con AWS CloudTrail	13/02/2018
AWS Artifact	Registrazione delle chiamate AWS Artifact API con AWS CloudTrail	27/01/2023
AWS Audit Manager	Registrazione AWS Audit Manager delle chiamate API con AWS CloudTrail	12/07/2020
AWS Auto Scaling	Registrazione delle chiamate AWS Auto Scaling API utilizzando CloudTrail	15/08/2018
AWS Scambio di dati B2B	Registrazione delle chiamate API AWS B2B Data Interchange utilizzando AWS CloudTrail	12/01/2023
AWS Backup	Registrazione AWS Backup delle chiamate API con AWS CloudTrail	02/04/2019
AWS Batch	Registrazione delle chiamate AWS Batch API con AWS CloudTrail	10/01/2018
Gestione dei costi e fatturazione AWS	Registrazione delle chiamate Gestione dei costi e fatturazione AWS API con AWS CloudTrail	06/07/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Billing Conductor	Registrazione delle chiamate AWS Billing Conductor API utilizzando AWS CloudTrail	03/12/2024
AWS BugBust	Registrazione BugBust delle chiamate API utilizzando CloudTrail	24/06/2021
AWS Certificate Manager	Uso di AWS CloudTrail	25/03/2016
AWS Clean Rooms	Registrazione delle chiamate API utilizzando AWS Clean RoomsAWS CloudTrail	21/03/2023
AWS Cloud Map	Registrazione delle chiamate API con AWS Cloud MapAWS CloudTrail	28/11/2018
AWS Cloud9	Registrazione delle chiamate AWS Cloud9 API con AWS CloudTrail	21/01/2019
AWS CloudFormation	Registrazione delle chiamate AWS CloudFormation API AWS CloudTrail	02/04/2014
AWS CloudHSM	Registrazione delle chiamate AWS CloudHSM API mediante AWS CloudTrail	08/01/2015
AWS CloudShell	Registrazione e monitoraggio AWS CloudShell	15/12/2020
AWS CloudTrail	AWS CloudTrail Riferimento API (tutte le chiamate CloudTrail API vengono registrate da.) CloudTrail	13/11/2013

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS CodeArtifact	Registrazione delle chiamate CodeArtifact API con AWS CloudTrail	10/06/2020
AWS CodeBuild	Registrazione delle chiamate API con AWS CodeBuildAWS CloudTrail	01/12/2016
AWS CodeCommit	Registrazione delle chiamate AWS CodeCommit API con AWS CloudTrail	11/01/2017
AWS CodeDeploy	Monitoraggio delle implementazioni con AWS CloudTrail	16/12/2014
AWS CodePipeline	Registrazione delle chiamate API con CodePipeline AWS CloudTrail	09/07/2015
AWS CodeStar	Registrazione delle chiamate AWS CodeStar API con AWS CloudTrail	14/06/2017
AWS CodeStar Notifiche	Registrazione delle chiamate API di AWS CodeStar notifica con AWS CloudTrail	05/11/2019
AWS Config	Registrazione delle chiamate AWS Config API con AWS CloudTrail	10/02/2015
AWS Catalogo di controllo	Registrazione delle chiamate API AWS di Control Catalog utilizzando AWS CloudTrail	08/04/2024

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Control Tower	Registrazione delle azioni con AWS Control TowerAWS CloudTrail	12/08/2019
AWS Data Pipeline	Registrazione delle chiamate AWS Data Pipeline API utilizzando AWS CloudTrail	02/12/2014
AWS Database Migration Service (AWS DMS)	Registrazione delle chiamate AWS Database Migration Service API utilizzando AWS CloudTrail	04/02/2016
AWS DataSync	Registrazione delle chiamate AWS DataSync API con AWS CloudTrail	26/11/2018
AWS Deadline Cloud	Registrazione delle chiamate Deadline Cloud API utilizzan do AWS CloudTrail	04/02/2024
AWS Device Farm	Registrazione AWS Device Farm delle chiamate API utilizzando AWS CloudTrail	13/07/2015
AWS Direct Connect	Registrazione delle chiamate AWS Direct Connect API AWS CloudTrail	08/03/2014
AWS Directory Service	Registrazione delle chiamate AWS Directory Service API mediante CloudTrail	14/05/2015
AWS Directory Service Dati	Registrazione delle chiamate API AWS Directory Service Data utilizzando AWS CloudTrail	18/09/2024

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Elastic Beanstalk (Elastic Beanstalk)	Utilizzo delle chiamate API Elastic Beanstalk con AWS CloudTrail	31/03/2014
AWS Elastic Disaster Recovery	Registrazione AWS Elastic Disaster Recovery delle chiamate API utilizzando AWS CloudTrail	17/11/2021
AWS Elemental MediaConnect	Registrazione AWS Elemental MediaConnect delle chiamate API con AWS CloudTrail	27/11/2018
AWS Elemental MediaConvert	Registrazione delle chiamate AWS Elemental MediaConvert API con CloudTrail	27/11/2017
AWS Elemental MediaLive	Registrazione delle chiamate MediaLive API con AWS CloudTrail	19/01/2019
AWS Elemental MediaPackage	Registrazione delle chiamate AWS Elemental MediaPackage API con AWS CloudTrail	21/12/2018
AWS Elemental MediaStore	Registrazione delle chiamate AWS Elemental MediaStore API con CloudTrail	27/11/2017
AWS Elemental MediaTailor	Registrazione delle chiamate AWS Elemental MediaTailor API con AWS CloudTrail	02/11/2019
AWS SMS di messaggistica per l'utente finale	Registrazione delle chiamate API SMS di messaggistica per l'utente AWS finale utilizzando AWS CloudTrail	10/10/2024

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Social di messaggistica per utenti finali	Registrazione delle chiamate all'API social di messaggistica per l'utente AWS finale utilizzando AWS CloudTrail	10/10/2024
AWS Risoluzione dell'entità	Registrazione delle chiamate API AWS Entity Resolution utilizzando A AWS CloudTrail	26/07/2023
AWS Fault Injection Service	Registra le chiamate API con AWS CloudTrail	15/03/2021
AWS Firewall Manager	Registrazione delle chiamate API con AWS Firewall ManagerAWS CloudTrail	05/04/2018
AWS Global Accelerator	Registrazione delle chiamate API AWS Global Accelerator con AWS CloudTrail	26/11/2018
AWS Glue	Operazioni di registrazione utilizzando AWS GlueAWS CloudTrail	07/11/2017
AWS Ground Station	Registrazione delle chiamate AWS Ground Station API con AWS CloudTrail	31/05/2019
AWS Health	Registrazione delle chiamate AWS Health API con AWS CloudTrail	21/11/2016
AWS Health Dashboard	Registrazione delle chiamate AWS Health API con AWS CloudTrail	01/12/2016

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS HealthImaging	Registrazione delle chiamate AWS HealthImaging API utilizzando AWS CloudTrail	26/07/2023
AWS HealthLake	Registrazione AWS HealthLake delle chiamate API con AWS CloudTrail	12/07/2020
AWS HealthOmics	Registrazione delle chiamate API utilizzando AWS HealthOmics AWS CloudTrail	29/11/2022
AWS IAM Identity Center	Registrazione delle chiamate API IAM Identity Center con AWS CloudTrail	07/12/2017
AWS IAM Identity Center — SCIM	Registrazione delle chiamate API di IAM Identity Center con AWS CloudTrail	28/10/2024
AWS Identity and Access Management (IAM)	Registrazione degli eventi IAM con AWS CloudTrail	13/11/2013
AWS IoT	Registrazione delle chiamate AWS IoT API con AWS CloudTrail	11/04/2016
AWS IoT Analisi	Registrazione delle chiamate all'API AWS IoT Analytics con AWS CloudTrail	23/04/2018
AWS IoT Events	Comprendere le AWS IoT Events voci dei file di registro	06/11/2019
AWS IoT Greengrass	Registrazione delle chiamate AWS IoT Greengrass API con AWS CloudTrail	29/10/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS IoT Greengrass V2	Registra le chiamate API AWS IoT Greengrass V2 con AWS CloudTrail	14/12/2020
AWS IoT SiteWise	Registrazione AWS IoT SiteWise delle chiamate API con AWS CloudTrail	29/04/2020
AWS Key Management Service (AWS KMS)	Registrazione delle chiamate AWS KMS API utilizzando AWS CloudTrail	12/11/2014
AWS Lake Formation	Registrazione delle chiamate AWS Lake Formation API utilizzando AWS CloudTrail	09/08/2019
AWS Lambda	Registrazione delle chiamate AWS Lambda API utilizzando AWS CloudTrail	Eventi di gestione: 09/04/2015 Eventi di dati: 30/11/2017
AWS Launch Wizard	Registrazione delle chiamate AWS Launch Wizard API utilizzando AWS CloudTrail	11/08/2023
AWS License Manager	Registrazione delle chiamate API di AWS License Manager con AWS CloudTrail	03/01/2019
Modernizzazione del mainframe AWS	Registrazione delle chiamate Modernizzazione del mainframe AWS API utilizzando AWS CloudTrail	08/06/2022
Integrazioni gestite per AWS IoT Device Management	Registrazione delle chiamate API di integrazioni gestite utilizzando AWS CloudTrail	03/03/2025

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Managed Services	Gestione dei log in AMS Accelerate	21/12/2016
Marketplace AWS Accordi	Registrazione delle chiamate API di Agreements utilizzando AWS CloudTrail	09/01/2023
Marketplace AWS Servizio di implementazione	Registrazione delle chiamate del servizio di Marketpla ce AWS distribuzione con CloudTrail	29/11/2023
Marketplace AWS Scoperta	Registrazione delle chiamate dell'API Marketplace AWS Discovery utilizzando AWS CloudTrail	15/12/2022
Marketplace AWS Servizio di misurazione	Registrazione delle chiamate Marketplace AWS API con AWS CloudTrail	08/22/2018
AWS Migration Hub	Registrazione delle chiamate API AWS Migration Hub con AWS CloudTrail	14/08/2017
AWS Migration Hub Viaggi	Registrazione delle chiamate API AWS Migration Hub Journeys con AWS CloudTrail	12/03/2024
Approvazione multipartitica	Registrazione delle chiamate API di approvazione multipart itiche utilizzando AWS CloudTrail	17/06/2025
AWS Network Firewall	Registrazione delle chiamate all'API con AWS Network FirewallAWS CloudTrail	17/11/2020

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS OpsWorks for Chef Automate	Registrazione AWS OpsWorks for Chef Automate delle chiamate API con AWS CloudTrail	07/16/2018
AWS OpsWorks for Puppet Enterprise	Registrazione OpsWorks per le chiamate API Puppet Enterprise con AWS CloudTrai l	07/16/2018
AWS OpsWorks Stacks	Registrazione delle chiamate API con AWS OpsWorks Stacks AWS CloudTrail	04/06/2014
Oracle Database@AWS	Registrazione delle chiamate API Oracle Database@ con AWSAWS CloudTrail	12/01/2024
AWS Organizations	Registrazione delle chiamate API con AWS Organizat ionsAWS CloudTrail	27/02/2017
AWS Outposts	Registrazione delle chiamate AWS Outposts API con AWS CloudTrail	02/04/2020
AWS Panorama	Riferimento API AWS Panorama	20/10/2021
AWS Payment Cryptography	Registrazione delle chiamate API utilizzando AWS Payment CryptographyAWS CloudTrail	06/08/2023
AWS 5G privato	Registrazione delle chiamate API 5G AWS private utilizzan do AWS CloudTrail	08/11/2022

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Private Certificate Authority (AWS Private CA)	Usando CloudTrail	04/04/2018
AWS Proton	Registrazione e monitoraggio AWS Proton	09/06/2021
AWS re:Post Privato	Registrazione delle chiamate API AWS re:Post private utilizzando AWS CloudTrail	26/11/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	Registrazione delle chiamate API con AWS RAMAWS CloudTrail	20/11/2018
Esploratore di risorse AWS	Registrazione delle chiamate Esploratore di risorse AWS API utilizzando AWS CloudTrail	11/07/2022
AWS Resource Groups	Registrazione e monitoraggio in Resource Groups	06/29/2018
AWS RoboMaker	Registrazione delle chiamate AWS RoboMaker API con AWS CloudTrail	01/16/2019
AWS Secrets Manager	Monitora l'uso dei tuoi segreti AWS Secrets Manager	05/04/2018
AWS Security Hub	Registrazione delle chiamate AWS Security Hub API con AWS CloudTrail	27/11/2018

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS Risposta agli incidenti di sicurezza	Registrazione delle chiamate all'API AWS Security Incident Response utilizzando AWS CloudTrail	12/01/2024
AWS Security Token Service (AWS STS)	Registrazione degli eventi IAM con AWS CloudTrail L'argomento IAM include informazioni per AWS STS.	13/11/2013
AWS Serverless Application Repository	Registrazione delle chiamate AWS Serverless Applicati on Repository API con AWS CloudTrail	20/02/2018
AWS Service Catalog	Registrazione delle chiamate API Service Catalog con AWS CloudTrail	06/07/2016
AWS Shield	Registrazione delle chiamate API Shield Advanced con AWS CloudTrail	08/02/2018
AWS Snowball Edge Edge	Registrazione delle chiamate API AWS Snowball Edge Edge con AWS CloudTrail	01/25/2019
AWS Step Functions	Registrazione delle chiamate AWS Step Functions API con AWS CloudTrail	01/12/2016
AWS Storage Gateway	Registrazione delle chiamate API Storage Gateway mediante AWS CloudTrail	16/12/2014

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
Supporto AWS	Registrazione delle chiamate Supporto AWS API con AWS CloudTrail	21/04/2016
Supporto Consigli (anteprima)	Registrazione delle chiamate all'API Supporto Recommendations con AWS CloudTrail	22/05/2024
AWS Systems Manager	Registrazione delle chiamate API con AWS Systems ManagerAWS CloudTrail	29/11/2017
AWS Systems Manager Incident Manager	Registrazione delle chiamate API di AWS Systems Manager Incident Manager utilizzando AWS CloudTrail	10/05/2021
AWS Costruttore di reti di telecomunicazioni (TNB)AWS	Registrazione delle chiamate API AWS Telco Network Builder utilizzando AWS CloudTrail	21/02/2023
AWS Transfer for SFTP	Registrazione AWS Transfer for SFTP delle chiamate API con AWS CloudTrail	01/08/2019
AWS Transit Gateway	Registrazione delle chiamate API per Transit Gateway con AWS CloudTrail	26/11/2018
AWS Trusted Advisor	Registrazione delle azioni della AWS Trusted Advisor console con AWS CloudTrail	22/10/2020
Accesso verificato da AWS	Registra Accesso verificato da AWS le chiamate API utilizzando AWS CloudTrail	27/04/2023

AWS Servizio	CloudTrail Argomenti	Il supporto è iniziato in data
AWS WAF	Registrazione AWS WAF delle chiamate API con AWS CloudTrail	28/04/2016
AWS Well-Architected Tool	Registrazione delle chiamate AWS Well-Architected Tool API con AWS CloudTrail	15/12/2020
AWS X-Ray	Registrazione delle chiamate API con AWS X-Ray CloudTrail	25/04/2018
Sistema di bilanciamento del carico elastico	AWS CloudTrail Registrazione per il Classic Load Balancer AWS CloudTrail e registrazione per l'Application Load Balancer	04/04/2014
Aggiornamenti Over-the-Air FreerTOS (OTA)	Registrazione delle chiamate API AWS IoT OTA con AWS CloudTrail	05/22/2019
Service Quotas (Quote di Servizio)	Registrazione delle chiamate API Service Quotas utilizzando AWS CloudTrail	24/06/2019

CloudTrail servizi non supportati

I servizi ancora in anteprima, non ancora rilasciati per la disponibilità generale (GA) o che non sono disponibili al pubblico APIs, non sono considerati supportati.

Inoltre, i seguenti AWS servizi ed eventi non sono supportati:

- AWS Import/Export

Per un elenco dei AWS servizi supportati, vedereAWS argomenti di servizio per CloudTrail.

Quote in AWS CloudTrail

Questa sezione descrive le quote di risorse (precedentemente denominate limiti) in. CloudTrail Per informazioni su tutte le quote in CloudTrail, vedere Quote di servizio in. Riferimenti generali di AWS

> **Note**
>
> CloudTrail non ha quote regolabili.

CloudTrail quote di risorse

La tabella seguente descrive le quote di risorse all'interno di. CloudTrail

Risorsa	Quota predefinita	Commenti
Percorsi per Regione	5	Il numero massimo di percorsi per. Regione AWS Nelle regioni ombra, per ottenere la metrica più recente sul conteggio delle risorse, chiama l'`ListTrails` API. Questa quota non può essere aumentata.
Datastore di eventi	10	Il numero massimo di archivi di dati di eventi per. Regione AWS Ciò include archivi dati di eventi a regione singola per la regione, archivi dati di eventi multiregionali in tutte le Regioni AWS aree e archivi dati di eventi dell'orga nizzazione. Ciò include i datastore di eventi in qualsiasi fase del ciclo di vita.

Risorsa	Quota predefinita	Commenti
		Nelle regioni ombra, per ottenere la metrica più recente sul conteggio delle risorse, chiama l'API. `ListEventDataStores` Questa quota non può essere aumentata.
Canali	25	Questa quota si applica ai canali utilizzati per le integrazioni di CloudTrail Lake con fonti di AWS eventi esterne e non si applica ai canali collegati ai servizi. Questa quota non può essere aumentata.
Dashboard per regione	100	Il numero massimo di dashboard personalizzate CloudTrail Lake per. Regione AWS Nelle regioni ombra, per ottenere la metrica più recente sul conteggio delle risorse, chiama l'`ListDashboards` API. Questa quota non può essere aumentata.

Risorsa	Quota predefinita	Commenti
Widget per dashboard	10	Questo numero massimo di widget per dashboard CloudTrail Lake. Questa quota non può essere aumentata.
Aggiornamenti simultanei della dashboard	1	Il numero massimo di aggiornamenti continui per dashboard. Questa quota non può essere aumentata.
Query simultanee	10	Il numero massimo di query in coda o in esecuzione che puoi eseguire contempor aneamente in Lake. CloudTrail Questa quota non può essere aumentata.
Eventi per richiesta PutAuditE vents	100	Puoi aggiungere fino a 100 eventi delle attività (o fino a 1 MB) per ciascuna richiesta `PutAuditEvents` . Questa quota non può essere aumentata.
Selettori di eventi	5 per trail	Questa quota non può essere aumentata.

Risorsa	Quota predefinita	Commenti
Selettori di eventi avanzati	500 Condizioni per tutti i selettori di eventi avanzati	Se un trail o un archivio di dati degli eventi utilizza selettori di eventi avanzati, è permesso un massimo di 500 valori totali per tutte le condizioni, in tutti i selettori di eventi avanzati. Questa quota non può essere aumentata.

Risorsa	Quota predefinita	Commenti
Risorse di dati nei selettori di eventi	250 in tutti i selettori di eventi in un trail	Se scegli di limitare gli eventi relativi ai dati utilizzando i selettori di eventi, il numero totale di risorse di dati non può superare 250 tra tutti i selettori di eventi di un trail. Il limite del numero di risorse in un singolo selettore di eventi è configura bile fino a un massimo di 250. Questo limite superiore è consentito solo se il numero totale di risorse di dati non è superiore a 250 in tutti i selettori di eventi. Esempi: • È consentito un trail con 5 selettori di eventi, ognuno configurato con 50 risorse di dati. (5*50=250) • È inoltre permesso un percorso con 5 selettori di eventi, 3 dei quali sono configurati con 50 risorse di dati, 1 dei quali è configura to con 99 risorse di dati e 1 dei quali è configurato con 1 risorsa di dati. ((3*50)+1 +99=250) • Non è consentito un trail configurato con 5 selettori di eventi, tutti configura ti con 100 risorse di dati. (5*100=500)

Risorsa	Quota predefinita	Commenti
		I selettori di eventi si applicano solo ai trail. Per gli archivi di dati degli eventi, è necessari o utilizzare i selettori di eventi avanzati. Questa quota non può essere aumentata. Il limite non si applica se scegli di registrare eventi di dati su tutte le risorse, ad esempio tutti i bucket S3 o tutte le funzioni Lambda.
Dimensioni dell'evento	Tutte le versioni degli eventi: gli eventi superiori a 256 KB non possono essere inviati ai registri CloudWatch Versione dell'evento 1.05 e successiva: limite delle dimensioni totali dell'evento di 256 KB	Amazon CloudWatch Logs e Amazon consentono EventBridge ciascuno una dimensione massima degli eventi di 256 KB. CloudTrai l non invia eventi superiori a 256 KB a CloudWatch Logs o. EventBridge A partire dalla versione dell'evento 1.05, gli eventi hanno una dimensione massima di 256 KB. Questo serve a prevenire lo sfruttame nto da parte di malintenzionati e a consentire che gli eventi vengano utilizzati da altri AWS servizi, come CloudWatch Logs and. EventBridge

Risorsa	Quota predefinita	Commenti
CloudTrail dimensione del file inviato ad Amazon S3	50 MB prima della compressione	Per eventi di gestione, dati e attività di rete, CloudTrail invia eventi a S3 in file gzip compressi. La dimensione massima del file prima della compressione è di 50 MB. Se abilitate durante il percorso, le notifiche di consegna dei log vengono inviate da Amazon SNS dopo l' CloudTrail invio dei file gzip a S3.

Quote di transazioni al secondo (TPS) in CloudTrail

Riferimenti generali di AWSElenca la quota di transazioni al secondo (TPS) per. AWS APIs La quota di transazioni al secondo (TPS) per un'API rappresenta il numero di richieste che è possibile effettuare al secondo per una determinata API senza subire limitazioni. Ad esempio, la quota TPS per l' CloudTrail `LookupEvents`API è 2.

Per informazioni sulla quota TPS per ogni CloudTrail API, vedi Quote di servizio in. Riferimenti generali di AWS

Guida introduttiva ai AWS CloudTrail tutorial

Se non lo conosci AWS CloudTrail, questi tutorial possono aiutarti a imparare a usare le sue funzionalità. Per utilizzare CloudTrail le funzionalità, devi disporre delle autorizzazioni adeguate. Questa pagina descrive le politiche gestite disponibili CloudTrail e fornisce informazioni su come concedere le autorizzazioni.

Esempi:

- Concedi le autorizzazioni di utilizzo CloudTrail
- Visualizza la cronologia degli eventi
- Crea un percorso per registrare gli eventi di gestione
- Crea un archivio dati di eventi per gli eventi di dati S3

Concedi le autorizzazioni di utilizzo CloudTrail

Per creare, aggiornare e gestire CloudTrail risorse come percorsi, archivi di dati di eventi e canali, devi concedere le autorizzazioni di utilizzo. CloudTrail Questa sezione fornisce informazioni sulle politiche gestite disponibili per CloudTrail.

> **Note**
>
> Le autorizzazioni concesse agli utenti per eseguire attività di CloudTrail amministrazione non sono le stesse autorizzazioni CloudTrail necessarie per inviare file di log ai bucket Amazon S3 o inviare notifiche ad argomenti di Amazon SNS. Per ulteriori informazioni su queste autorizzazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.
> Se configuri l'integrazione con Amazon CloudWatch Logs, richiede CloudTrail anche un ruolo che può assumere per fornire eventi a un gruppo di log di Amazon CloudWatch Logs. È necessario creare il ruolo che CloudTrail utilizza. Per ulteriori informazioni, consulta Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail e Invio di eventi ai registri CloudWatch .

Le seguenti politiche AWS gestite sono disponibili per CloudTrail:

- AWSCloudTrail_FullAccess— Questa policy fornisce l'accesso completo alle CloudTrail azioni sulle CloudTrail risorse, come percorsi, archivi di dati sugli eventi e canali. Questa politica fornisce le

autorizzazioni necessarie per creare, aggiornare ed eliminare CloudTrail percorsi, archivi dati di eventi e canali.

Questa policy fornisce anche le autorizzazioni per gestire il bucket Amazon S3, il gruppo di log CloudWatch per Logs e un argomento Amazon SNS per un trail. Tuttavia, la policy `AWSCloudTrail_FullAccess` gestita non fornisce le autorizzazioni per eliminare il bucket Amazon S3, il gruppo di log CloudWatch per Logs o un argomento di Amazon SNS. Per informazioni sulle politiche gestite per altri AWS servizi, consulta la Managed Policy Reference Guide AWS .

> **Note**
>
> Il AWSCloudTrail_FullAccessla politica non è pensata per essere condivisa ampiamente tra i tuoi Account AWS. Gli utenti con questo ruolo hanno la possibilità di disattivare o riconfigurare le funzioni di auditing più sensibili e importanti negli Account AWS. Per questo motivo, è necessario applicare questa policy solo agli amministratori degli account. È necessario controllare e monitorare attentamente l'uso di questa policy.

- AWSCloudTrail_ReadOnlyAccess— Questa politica concede le autorizzazioni per visualizzare la CloudTrail console, inclusi gli eventi recenti e la cronologia degli eventi. Questa policy consente inoltre di visualizzare percorsi, datastore di eventi e canali esistenti. I ruoli e gli utenti con questa policy possono scaricare la cronologia degli eventi, ma non possono creare o aggiornare percorsi, datastore di eventi o canali.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in: AWS IAM Identity Center

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Visualizza la cronologia degli eventi

Questa sezione descrive come utilizzare la pagina della cronologia degli CloudTrail eventi sulla CloudTrail console per visualizzare gli ultimi 90 giorni di gestione degli eventi di gestione Account AWS per quelli correnti Regione AWS.

Per visualizzare la cronologia degli eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi). Consultare un elenco filtrato di eventi, con gli eventi più recenti visualizzati per primi. Il filtro predefinito per gli eventi è di Read-only (Sola lettura), impostato su false (Falso). È possibile rimuovere il filtro scegliendo la X alla sua destra. Puoi cercare gli eventi nella Cronologia degli eventi filtrando gli eventi in base a un singolo attributo.

3. Scegli un attributo in base al quale filtrare e inserisci il valore completo dell'attributo. CloudTrail non è possibile filtrare in base a un valore parziale. Ad esempio, per visualizzare tutti gli eventi di accesso alla console, scegli il filtro Nome evento e specifica ConsoleLoginil valore dell'attributo.

   Oppure, per visualizzare gli eventi di CloudTrail gestione recenti, scegliete Origine evento e specificate`cloudtrail.amazonaws.com`. Per informazioni sugli eventi a cui un servizio si registra CloudTrail, consulta l'API Reference del servizio.

4. Per visualizzare un evento di gestione specifico, scegli il nome dell'evento. Nella pagina dei dettagli dell'evento, è possibile visualizzare i dettagli dell'evento, visualizzare le risorse di riferimento e visualizzare il record dell'evento.
5. Per confrontare gli eventi, seleziona fino a cinque eventi compilando le relative caselle di controllo sul margine sinistro della tabella Event history (Cronologia eventi). È possibile visualizzare i dettagli degli eventi selezionati side-by-side nella tabella Confronta i dettagli degli eventi.

6. È possibile salvare la cronologia eventi scaricandola come file in formato JSON o CSV. Il download della cronologia eventi può richiedere alcuni minuti.

Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Crea un percorso per registrare gli eventi di gestione

Per il primo itinerario, consigliamo di creare un percorso che registri tutti gli eventi di gestione e non registri gli eventi relativi ai dati o gli eventi Insights. Esempi di eventi di gestione includono eventi di sicurezza come gli eventi IAM `CreateUser` e `AttachRolePolicy`, eventi delle risorse come `RunInstances` e `CreateBucket` e molto altro. Creerai un bucket Amazon S3 in cui archivierai i file di registro per il percorso come parte della creazione del percorso nella console. CloudTrail

> **Note**
>
> AWS Control Tower imposta un nuovo evento di gestione del CloudTrail trail logging quando si configura una landing zone. È un percorso a livello di organizzazione, il che significa che registra tutti gli eventi di gestione per l'account di gestione e tutti gli account dei membri dell'organizzazione. Per ulteriori informazioni, vedere Informazioni sull'accesso nella AWS Control Tower Guida per l'utente.AWS CloudTrail
> Questo tutorial presuppone che si stia creando il primo percorso. A seconda del numero di percorsi presenti nell' AWS account e della configurazione di tali percorsi, la procedura seguente potrebbe comportare o meno dei costi. CloudTrail archivia i file di log in un bucket Amazon S3, il che comporta dei costi. Per ulteriori informazioni sui prezzi, consultare Prezzi di AWS CloudTrail e Prezzi di Amazon S3.

Per creare un trail

1. Accedi a AWS Management Console e apri la console all' CloudTrail indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Nel selettore della regione, scegli la AWS regione in cui desideri creare il percorso. Questa è la regione di origine del percorso.

> **Note**
>
> La regione di origine è l'unica Regione AWS in cui è possibile aggiornare il percorso dopo la sua creazione.

3. Nella home page del CloudTrail servizio, nella pagina Percorsi o nella sezione Percorsi della pagina Dashboard, scegli Crea percorso.
4. Nel Trail name (Nome trail), dai un nome al tuo percorso, ad esempio *`management-events`*. Come best practice, è consigliabile utilizzare un nome che identifichi in modo rapido lo scopo del percorso. In questo caso, si crea un percorso che registra gli eventi di gestione.
5. Lascia l'impostazione predefinita per Abilita per tutti gli account della mia organizzazione. Questa opzione non sarà disponibile per la modifica, a meno che siano stati configurati account in Organizations.
6. Per Storage location (Posizione di archiviazione), scegliere Create new S3 bucket (Crea nuovo bucket S3) per creare un bucket. Quando crei un bucket, CloudTrail crea e applica le politiche del bucket richieste. Se scegli di creare un nuovo bucket S3, la tua policy IAM deve includere l'autorizzazione per l'`s3:PutEncryptionConfiguration`azione perché per impostazione predefinita la crittografia lato server è abilitata per il bucket. Assegna al bucket un nome che lo renda facile da identificare.

   Per facilitare la ricerca dei log, crea una nuova cartella (nota anche come prefisso) in un bucket esistente per archiviare i log. CloudTrail

   > **Note**
   >
   > Il nome del bucket Amazon S3 deve essere univoco a livello globale. Per ulteriori informazioni, consulta Regole per la denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

7. Deselezionare la casella di controllo per disabilitare Log file SSE-KMS encryption (Crittografia SSE-KMS dei file di log). Per impostazione predefinita, i file di log sono crittografati con la crittografia SSE-S3. Per ulteriori informazioni su questa impostazione, consulta Uso della crittografia lato server con le chiavi gestite di Amazon S3 (SSE-S3).
8. Lascia le impostazioni predefinite in Additional settings (Impostazioni aggiuntive).
9. Lascia le impostazioni predefinite per i log. CloudWatch Per ora, non inviare log ad Amazon CloudWatch Logs.

10. (Facoltativo) In Tags, puoi aggiungere fino a 50 coppie di chiavi di tag per aiutarti a identificare, ordinare e controllare l'accesso al tuo percorso. I tag possono aiutarti a identificare i CloudTrail percorsi e altre risorse, come i bucket Amazon S3 che contengono CloudTrail file di registro. Ad esempio, è possibile allegare un tag con il nome **`Compliance`** e il valore **`Auditing`**.

> **Note**
>
> Sebbene sia possibile aggiungere tag ai percorsi quando li si crea nella CloudTrail console e creare un bucket Amazon S3 per archiviare i file di registro nella CloudTrail console, non è possibile aggiungere tag al bucket Amazon S3 dalla console. CloudTrail Per ulteriori informazioni sulla visualizzazione e la modifica delle proprietà di un bucket Amazon S3, inclusa l'aggiunta di tag a un bucket, consultare la Guida per l'utente di Amazon S3.

Quando hai terminato la creazione di tag, seleziona Next (Successivo).

11. Nella pagina Choose log events (Seleziona eventi di log), seleziona i tipi di evento da registrare. Per questo percorso, mantieni le impostazioni predefinite, Management events (Eventi di gestione). Nell'area Management events (Eventi di gestione), scegli di registrare sia gli eventi Read (Lettura) che Write (Scrittura), se non sono già selezionati. Lascia vuote le caselle di controllo Escludi AWS KMS eventi ed Escludi eventi Amazon RDS Data API per registrare tutti gli eventi di gestione.

12. Lascia le impostazioni predefinite per gli eventi Data, gli eventi Insights e gli eventi di attività di rete. Questo percorso non registrerà alcun evento relativo ai dati, eventi Insights o eventi di attività di rete. Scegli Next (Successivo).
13. Nella pagina Review and create (Verifica e crea), rivedere le impostazioni selezionate per il percorso. Scegliere Edit (Modifica) in una sezione per tornare indietro e apportare modifiche. Quando si è pronti per creare il percorso, scegliere Create trail (Crea percorso).
14. La pagina Trails (Percorsi) mostra il nuovo percorso nella tabella. Tenere presente che il percorso è impostato su Multi-region trail (Percorso multiregione) per impostazione predefinita e che la registrazione è attivata per il percorso per impostazione predefinita.

Per ulteriori informazioni sui sentieri, vedereLavorare con i CloudTrail sentieri.

Visualizzare i file di log

Entro una media di circa 5 minuti dalla creazione del primo trail, CloudTrail invia il primo set di file di log al bucket Amazon S3 per il percorso. È possibile esaminare questi file e le informazioni che contengono.

> **Note**
>
> CloudTrail in genere consegna i log entro una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail.
> Se configuri male il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterai di recapitare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti ai costi standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Visualizzazione dei file di log

1. Accedi a e apri la console all'indirizzo. AWS Management Console CloudTrail https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione selezionare Trails (Percorso). Nella pagina Percorsi, trova il nome del percorso che hai appena creato (nell'esempio,*management-events*).
3. Nella riga del percorso, scegli il valore per il bucket S3.
4. La console Amazon S3 si apre e mostra due cartelle per il bucket: e. `CloudTrail-Digest` `CloudTrail` Scegli la CloudTrailcartella per visualizzare i file di registro.
5. Se hai creato un percorso multiregionale, esiste una cartella per ogni Regione AWS percorso. Scegli la cartella in Regione AWS cui desideri rivedere i file di registro. Ad esempio, per esaminare i file di log per la regione Stati Uniti orientali (Ohio), scegliere us-east-2.
6. Passare alla struttura della cartella del bucket, all'anno, al mese e al giorno in cui si desidera esaminare i log di attività in quella regione. In quel giorno, sono presenti molti file. Il nome dei file inizia con il tuo Account AWS ID e termina con l'estensione`.gz`. Ad esempio, se l'ID del tuo account è*123456789012*, vedrai file con nomi simili a questo: *123456789012* _ _ CloudTrail *us-east-2* _ *20240512T0000Z_EXAMPLE* .json.gz.

Per visualizzare questi file, è possibile scaricarli, decomprimerli e quindi visualizzarli in un editor di testo normale o un visualizzatore file JSON. Alcuni browser, inoltre, supportano la visualizzazione dei file .gz e JSON direttamente. Consigliamo di usare un visualizzatore JSON, che semplifica l'analisi delle informazioni del file di log CloudTrail .

Crea un archivio dati di eventi per gli eventi di dati S3

È possibile creare un archivio dati di eventi per registrare CloudTrail eventi (eventi di gestione, eventi relativi ai dati), eventi CloudTrail Insights, AWS Audit Manager prove, elementi di AWS Config configurazione o non AWS eventi.

Quando crei un archivio dati di eventi per gli eventi di dati, scegli i tipi di risorse Servizi AWS e i tipi di risorse per i quali desideri registrare gli eventi relativi ai dati. Per informazioni sugli Servizi AWS eventi relativi ai dati di registro, consultaEventi di dati.

Questa procedura dettagliata mostra come creare un data store per eventi di dati di Amazon S3. In questo tutorial, invece di registrare tutti gli eventi di dati di Amazon S3, sceglieremo un modello di selettore di log personalizzato per registrare gli eventi solo quando un oggetto viene eliminato da un bucket S3 specifico.

Creazione di un datastore di eventi per eventi di dati S3

1. Accedi a AWS Management Console e apri la console all' CloudTrail indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configura il data store degli eventi, in Dettagli generali, assegna un nome al tuo event data store, ad esempio`s3-data-events-eds`. Come best practice, è consigliabile utilizzare un nome che identifichi in modo rapido lo scopo del datastore di eventi. Per informazioni sui requisiti di CloudTrail denominazione, vedereRequisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

- Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a prezzi pay-as-you-go convenienti. Questa è l'opzione predefinita.
  - Periodo di conservazione predefinito: 366 giorni
  - Periodo di conservazione massimo: 3.653 giorni
- Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
  - Periodo di conservazione predefinito: 2.557 giorni
  - Periodo di conservazione massimo: 2.557 giorni

6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

   CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

7. (Facoltativo) In Crittografia, scegli se vuoi crittografare il datastore di eventi utilizzando la tua chiave KMS. Per impostazione predefinita, tutti gli eventi in un Event Data Store sono crittografati CloudTrail utilizzando una chiave KMS che AWS possiede e gestisce per te.

   Per abilitare la crittografia utilizzando la tua chiave KMS, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno personalizzato oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/`*`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia CloudTrail dei log. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

> **Note**
>
> Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.
   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.
   c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato possono eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) In Tag, aggiungi uno o più tag personalizzati (coppie chiave-valore) al datastore di eventi. I tag possono aiutarti a identificare i tuoi archivi di dati sugli CloudTrail eventi. Ad esempio, è possibile allegare un tag con il nome **`stage`** e il valore **`prod`**. Puoi usare i tag per limitare l'accesso al datastore di eventi. Puoi utilizzare questi tag anche per tenere traccia dei costi di query e importazione per il datastore di eventi.

    Per informazioni su come controllare utilizzare i tag per monitorare i costi, consulta Creazione di tag di allocazione dei costi definiti dall'utente per i data store di CloudTrail eventi Lake. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un datastore di eventi in base ai tag, consulta Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per informazioni su come utilizzare i tag in AWS, consulta Tagging your AWS resources nella Tagging AWS Resources User Guide.

11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Scegli eventi, lascia le selezioni predefinite per Tipo di evento.

13. Per CloudTrail gli eventi, scegli Data events e deseleziona Management events. Per ulteriori informazioni sugli eventi di dati, consulta Registrazione degli eventi di dati.

14. Lascia l'impostazione predefinita per Copia eventi di percorso. Puoi usare questa opzione per copiare gli eventi di percorso nel datastore di eventi. Per ulteriori informazioni, consulta Copia di eventi traccia in un archivio dati degli eventi.
15. Scegli Abilita per tutti gli account della mia organizzazione se si tratta di un datastore di eventi dell'organizzazione. Questa opzione non sarà disponibile per la modifica, a meno che non ci siano già degli account in AWS Organizations.
16. Per Impostazioni aggiuntive lascia le selezioni predefinite. Per impostazione predefinita, un Event Data Store raccoglie gli eventi per tutti Regioni AWS e inizia a importarli al momento della creazione.
17. Per Eventi di dati, effettua le seguenti selezioni:

    a. In Tipo di risorsa, scegli S3. Il tipo di risorsa identifica la risorsa Servizio AWS e su cui vengono registrati gli eventi relativi ai dati.

    b. In Modello di selettore di log, scegli Personalizzato. Scegliendo Personalizzato potrai definire un selettore di eventi personalizzato da filtrare in base ai campi `eventName`, `resources.ARN` e `readOnly`. Per informazioni su questi campi, consulta l'AWS CloudTrail API AdvancedFieldSelectorReference.

    c. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio «Registra le chiamate DeleteObject API per uno specifico bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

    d. Nei selettori di eventi avanzati, creeremo il selettore di eventi personalizzato per filtrare i campi and. `eventName` `resources.ARN` I selettori di eventi avanzati per un archivio di dati degli eventi funzionano allo stesso modo dei selettori di eventi avanzati applicati a un percorso. Per ulteriori informazioni su come creare selettori di eventi avanzati, consultare Registrazione di eventi di dati con i selettori di eventi avanzati.

        i. Per Campo scegli eventName. Per Operatore, scegli equals. In Valore, specifica **`DeleteObject`**. Scegli + Campo per filtrare in base a un altro campo.

        ii. Per Campo, scegli resources.ARN. Per Operatore, scegli StartsWith. Per Value, inserisci l'ARN per il tuo bucket (ad esempio, arn:aws:s3:::). *`amzn-s3-demo-bucket`*

Per maggiori informazioni su come ottenere l'ARN, consulta Risorse di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

18. Scegli Next (Successivo) per rivedere le scelte effettuate.
19. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
20. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.

    Da questo momento in poi, l'archivio di dati degli eventi cattura gli eventi che corrispondono ai suoi selettori di eventi avanzati. Gli eventi che si sono verificati prima della creazione dell'archivio di dati degli eventi non si trovano all'interno dell'archivio, a meno che tu non si abbia scelto di copiare gli eventi di trail esistenti.

Ora è possibile eseguire query sul nuovo datastore di eventi. Per informazioni sulla modalità di visualizzazione ed esecuzione di query di esempio, consulta Visualizza query di esempio con la console CloudTrail .

Per ulteriori informazioni su Lake, vedere. CloudTrail Lavorare con AWS CloudTrail Lake

Visualizzazione dei CloudTrail costi e dell'utilizzo con AWS Cost Explorer

Questa sezione descrive come visualizzare i CloudTrail costi e l'utilizzo utilizzando AWS Cost Explorer. Cost Explorer ti dà la possibilità di visualizzare, comprendere e gestire i AWS costi e l'utilizzo nel tempo.

Per informazioni dettagliate sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Per visualizzare CloudTrail costi e utilizzo con Cost Explorer

1. Accedi AWS Management Console e apri la console Cost Explorer a https://console.aws.amazon.com/cost-management/home#/custom.
2. In Ora, scegli l'intervallo di date che desideri analizzare.
3. In Raggruppa per, per Dimensione, scegli Tipo di utilizzo.
4. In Filtri, per Servizio, scegli CloudTrail.

L'immagine seguente mostra un esempio di rapporto sui costi filtrato CloudTrail e raggruppato per tipo di utilizzo.

Controlla il tipo di utilizzo per vedere quali CloudTrail funzionalità hanno generato i costi maggiori. Ogni tipo di utilizzo inizia con il codice relativo al Regione AWS luogo in cui è stato effettuato l'addebito.

La tabella seguente descrive i tipi di CloudTrail utilizzo per ciascuna CloudTrail funzionalità.

CloudTrail caratteristica	Tipo di utilizzo	Descrizione
CloudTrail sentieri	`region-FreeEventsRecorded`	La prima copia degli eventi gestionali consegnata

CloudTrail caratteristica	Tipo di utilizzo	Descrizione
		gratuitamente a un Regione AWS.
CloudTrail sentieri	*region*-PaidEventsRecorded	Il costo per le copie aggiuntive e degli eventi di gestione consegnate a un Regione AWS.
CloudTrail sentieri	*region*-DataEventsRecorded	Il costo per l'invio di eventi relativi ai dati a un Regione AWS. Gli eventi relativi ai dati comportano sempre costi.
CloudTrail sentieri	*region*-NetworkEventsRecorded	Il costo per l'invio di eventi relativi alle attività di rete a un Regione AWS. Gli eventi di attività di rete sono sempre a pagamento.

CloudTrail caratteristica	Tipo di utilizzo	Descrizione
CloudTrail Lago	*region*-Ingestion-Bytes	L'addebito per l'inserimento di eventi in un archivio dati di eventi CloudTrail Lake utilizzando l'opzione di prezzo di conservazione per sette anni. I prezzi di importazione si basano sul volume di dati importati e sono gli stessi per tutti i tipi di eventi.
CloudTrail Lago	*region*-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	L'addebito per l'inserimento di eventi di CloudTrail dati, eventi di attività di rete ed eventi di gestione in un data store di eventi CloudTrail Lake utilizzando l'opzione di prezzo di conservazione estendibile di un anno.

CloudTrail caratteristica	Tipo di utilizzo	Descrizione
CloudTrail Lago	`region-Ingestion-Bytes-1yearstore-Other-data-sources`	L'addebito per l'acquisizione di altre fonti di eventi in un data store di eventi CloudTrail Lake utilizzando l'opzione di prezzo di conservazione estendibile di un anno. Ciò include eventi CloudTrail Insights, elementi di configurazione da AWS Config, prove da AWS Audit Manager, CloudTrail log storici (non compressi) importati da S3 ed eventi esterni a. AWS

CloudTrail caratteristica	Tipo di utilizzo	Descrizione
CloudTrail Lago	`region-QueryScanned-Bytes`	L'addebito per l'esecuzione di domande su CloudTrail Lake. Quando si eseguono query in CloudTrail Lake, vengono addebitati addebiti in base alla quantità di dati ottimizzati e compressi scansionati.
CloudTrail Approfondimenti	`region-InsightsEvents`	L'addebito per gli eventi CloudTrail Insights. Per gli eventi Insights, vengono addebitati addebiti in base al numero di eventi di gestione analizzati per tipo di Insight. Per ulteriori informazioni, consulta Costi per gli eventi Insights.

Utilizzo Budget AWS per gestire i costi

Budget AWS una funzionalità di Gestione dei costi e fatturazione AWS, consente di impostare budget personalizzati che avvisano l'utente quando i costi o l'utilizzo superano (o si prevede che superino) l'importo preventivato.

La creazione di un budget in CloudTrail base all'utilizzo Budget AWS è una best practice consigliata e può aiutarti a tenere traccia delle tue spese. CloudTrail I budget basati sui costi aiutano a promuovere la consapevolezza di quanto potrebbe esservi fatturato per il vostro utilizzo. CloudTrail Gli avvisi di budget inviano una notifica quando la fattura raggiunge una soglia definita dall'utente. Quando ricevi un avviso di budget, puoi apportare modifiche prima della fine del ciclo di fatturazione per gestire i costi.

> **Note**
>
> Sebbene sia possibile applicare tag ai CloudTrail percorsi, attualmente AWS Billing non è possibile utilizzare i tag applicati ai percorsi per l'allocazione dei costi. Cost Explorer può mostrare i costi per i data store di eventi CloudTrail Lake e per il CloudTrail servizio nel suo complesso.

Per iniziare a usare AWS Budgets Gestione dei costi e fatturazione AWS, apri e scegli Budgets nella barra di navigazione a sinistra. Ti consigliamo di configurare gli avvisi sul budget quando crei un budget per tenere traccia delle spese. CloudTrail Per ulteriori informazioni su come utilizzare i AWS budget, consulta Gestione dei costi con Budget AWS e Best practice per. Budget AWS

Creazione di tag di allocazione dei costi definiti dall'utente per i data store di CloudTrail eventi Lake

Puoi creare tag di allocazione dei costi definiti dall'utente per tenere traccia dei costi di query e ingestione per i tuoi data store di eventi Lake. CloudTrail Un tag di allocazione dei costi è una coppia chiave-valore che può essere associata a un datastore di eventi. Dopo aver attivato i tag di allocazione dei costi, AWS utilizza i tag per organizzare i costi delle risorse nel rapporto di allocazione dei costi.

- Per creare tag nella console, consulta la fase 9 della procedura Per creare un archivio dati per CloudTrail gli eventi.

- Per creare tag utilizzando l' CloudTrail API, consulta CreateEventDataStoreе AddTagsnell'AWS CloudTrail API Reference.
- Per creare tag utilizzando AWS CLI, consulta create-event-data-storeе aggiungi tag nel AWS CLI Command Reference.

Per ulteriori informazioni sull'attivazione dei tag, consulta Attivazione dei tag di allocazione dei costi definiti dall'utente.

Gestione dei costi dei CloudTrail percorsi

È possibile configurare e gestire i CloudTrail percorsi in modo da acquisire i dati necessari pur rimanendo convenienti. Per ulteriori informazioni sui CloudTrail prezzi, consulta AWS CloudTrail la sezione Prezzi.

Configurazione dei percorsi

CloudTrail offre flessibilità nel modo in cui configuri i percorsi nel tuo account. Alcune decisioni prese durante il processo di configurazione richiedono di comprendere l'impatto sulla fattura CloudTrail . Di seguito sono elencati alcuni esempi di come le configurazioni dei trail possono influenzare la fattura CloudTrail .

Creazione di più trail

La prima copia degli eventi gestionali all'interno di ciascuna regione viene consegnata gratuitamente. Ad esempio, se il tuo account ha 2 percorsi in una singola regione, un percorso in entrata `us-east-1` e un altro in entrataus`-west-2`, non ci sono CloudTrail costi perché c'è un solo evento di registrazione dei percorsi in ogni rispettiva regione. Tuttavia, se il tuo account ha un percorso multiregionale e un percorso a regione singola aggiuntivo, il percorso a regione singola comporterà dei costi perché il percorso multiregionale registra già gli eventi in ogni regione.

Se crei più percorsi che offrono gli stessi eventi di gestione ad altre destinazioni, tali consegne successive comportano dei costi. CloudTrail È possibile eseguire questa operazione per consentire a diversi gruppi di utenti (ad esempio sviluppatori, personale addetto alla sicurezza e revisori IT) di ricevere le proprie copie dei file di log. Per quanto riguarda gli eventi relativi ai dati, tutte le consegne comportano dei costi, inclusa la prima CloudTrail .

Quando crei più trail, è particolarmente importante avere familiarità con i log e comprendere i tipi e i volumi di eventi generati dalle risorse nel tuo account. In questo modo è possibile prevedere

il volume di eventi associati a un account e pianificare i costi del trail. Ad esempio, l'utilizzo della crittografia lato server AWS KMS gestita (SSE-KMS) sui bucket S3 può comportare un gran numero di eventi di gestione. AWS KMS CloudTrail I costi possono anche essere influenzati da volumi maggiori di eventi su più trail.

Per limitare il numero di eventi registrati sul tuo percorso, puoi filtrare gli eventi Amazon RDS Data API selezionando AWS KMS Escludi eventi o Escludi AWS KMS eventi Amazon RDS Data API nelle pagine Crea percorso o Aggiorna percorso. Quando utilizzi selettori di eventi di base, puoi filtrare solo gli eventi di gestione. Tuttavia, puoi utilizzare i selettori di eventi avanzati per filtrare sia gli eventi di gestione che gli eventi di dati.

È possibile utilizzare selettori di eventi avanzati per includere o escludere eventi di dati, in modo da registrare solo gli eventi di dati di interesse. Per ulteriori informazioni, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.

È possibile utilizzare selettori di eventi avanzati per includere o escludere gli eventi di attività di rete in base ai `vpcEndpointId` campi `eventName` `resources.typeresources.ARN`,`errorCode`,, e, in modo da registrare solo gli eventi relativi ai dati di interesse. Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.

Per ulteriori informazioni sulla creazione e l'aggiornamento di un percorso, consulta Creazione di un percorso con la CloudTrail console o Aggiornamento di un percorso con la CloudTrail console in questa guida.

AWS Organizations

Quando configuri un percorso Organizations con CloudTrail, CloudTrail replica il percorso su ogni account membro all'interno dell'organizzazione. Il nuovo trail viene creato in aggiunta a qualsiasi trail esistente negli account membri. Assicurati che la configurazione del trail principale corrisponda a come desideri che i trail siano configurati per tutti gli account all'interno di un'organizzazione, perché la configurazione del trail principale si propaga a tutti gli account.

Poiché Organizations crea un percorso in ogni account membro, un singolo account membro che crea un percorso aggiuntivo per raccogliere gli stessi eventi di gestione del percorso Organizations raccoglie una seconda copia degli eventi. L'account viene addebitato per la seconda copia. Analogamente, se un account dispone di un percorso multi-regione e crea un secondo percorso in una singola regione per raccogliere gli stessi eventi di gestione del percorso multi-regione, il percorso nella singola regione distribuisce una seconda copia degli eventi. La seconda copia comporta dei costi.

Consulta anche

- Prezzi di AWS CloudTrail
- Gestisci i costi con Budget AWS
- Nozioni di base su Esploratore dei costi
- Preparazione per la creazione di un percorso per la tua organizzazione

Gestione dei costi CloudTrail del lago

AWS CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake sono a pagamento. È possibile configurare gli archivi dati degli eventi in modo da acquisire i dati necessari pur rimanendo convenienti. Per informazioni sui prezzi di CloudTrail , consulta la pagina dei prezzi di AWS CloudTrail.

Argomenti

- Opzioni di prezzo del datastore di eventi
- Comprensione delle tariffe CloudTrail del lago
- Consigli su come ridurre i costi
- Consulta anche

Opzioni di prezzo del datastore di eventi

Quando crei un datastore di eventi, scegli l'opzione di prezzo che desideri utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il datastore di eventi.

Nella tabella seguente vengono descritte le opzioni di prezzo disponibili. La tabella mostra l'Opzione di prezzo nella console e il valore `BillingMode` corrispondente per l'API ed elenca il periodo di conservazione predefinito e quello massimo per ciascuna opzione.

Opzione di prezzo (console)	BillingMode (API)	Descrizione
Prezzo per la conservazione estendibile di un anno	`EXTENDABLE_RETENTION_PRICING`	Consigliato se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Questa opzione è consigliata anche se il datastore di eventi raccoglie elementi di configurazione di AWS Config , prove di Gestione Audit ed eventi dall'esterno di AWS. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza costi aggiuntivi nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita. Periodo di conservazione predefinito: 366 giorni Periodo di conservazione massimo: 3.653 giorni
Prezzo per la conservazione di sette anni	`FIXED_RETENTION_PRICING`	Consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi. Periodo di conservazione predefinito: 2.557 giorni Periodo di conservazione massimo: 2.557 giorni

Comprensione delle tariffe CloudTrail del lago

Le tabelle seguenti forniscono informazioni su come gli archivi e le query di dati sugli eventi di CloudTrail Lake comportano costi. Per informazioni sui prezzi di CloudTrail , consulta la pagina dei prezzi di AWS CloudTrail.

Tipo di costo	Come vengono addebitati i costi
Importazione dei dati (dati non compressi)	Per CloudTrail Lake, paghi in base ai dati non compressi importati. L'opzione di prezzo per il datastore di eventi determina il costo dell'importazione degli eventi: • Prezzo per la conservazione estendibile di un anno: offre un prezzo di importazione basato sul tipo di evento. • Prezzo per la conservazione di sette anni: offre un prezzo di importazione basato sul volume dei dati importati. Si ha un maggiore risparmio quando il volume dei dati importati mensilmente supera i 25 TB. Copia degli eventi del percorso Quando copi gli eventi del trail su CloudTrail Lake, CloudTrail decomprime i log archiviati in formato gzip (compresso). Quindi CloudTrail copia gli eventi contenuti nei log nel tuo archivio dati degli eventi. La dimensione dei dati non compressi potrebbe essere maggiore della dimensione di archiviazione effettiva di Amazon S3. Per avere una stima generale della dimensione dei dati non compressi, moltiplica la dimensione dei log nel bucket S3 per 10. **Note** CloudTrail non copierà un evento se l'ora dell'evento è precedente al periodo di conservazione specificato. Per determinare il periodo di conservazione corretto, calcola la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni per cui desideri conservare

Tipo di costo	Come vengono addebitati i costi
	gli eventi nel datastore eventi, come dimostrato nell'equazione seguente: Periodo di conservazione = *oldest-event-in-days* + *number-days-to-retain* Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.
Conservazione dei dati (dati ottimizzati e compressi)	CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati compressi. Il periodo di conservazione di un Event Data Store determina per quanto tempo i dati degli eventi vengono conservati nell'Event Data Store. CloudTrail Lake determina se conservare un evento controllando se l'ora dell'evento rientra nel periodo di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando la durata dell'evento è precedente a 90 giorni. Per i datastore di eventi che utilizzano l'opzione Prezzo per la conservazione di sette anni, l'archiviazione è inclusa nel prezzo di importazione senza costi aggiuntivi. Per i datastore di eventi che utilizzano l'opzione Prezzo per la conservazione estendibile di un anno, l'archiviazione è inclusa nel prezzo di importazione senza costi aggiuntivi per i primi 366 giorni (periodo di conservazione predefinito). Dopo 366 giorni, lo storage viene offerto pay-as-you-pricing e addebitato in base ai dati ottimizzati e compressi presenti nell'Event Data Store.

Tipo di costo	Come vengono addebitati i costi
Esecuzione di query in CloudTrail Lake (dati ottimizzati e compressi)	Quando esegui query in CloudTrail Lake, paghi in base alla quantità di dati ottimizzati e compressi scansionati.

Consigli su come ridurre i costi

Questa sezione fornisce consigli su come ridurre i costi quando si lavora con Lake. CloudTrail

Scegli un'opzione di prezzo in base al tipo di eventi raccolti dal datastore di eventi e all'importazione mensile prevista

Durante la creazione di un datastore di eventi, scegli un'opzione di prezzo in base al tipo di eventi raccolti dal datastore e all'importazione mensile prevista.

Se prevedi di importare meno di 25 TB di dati al mese e cerchi un periodo di conservazione flessibile fino a 10 anni, scegli l'opzione Prezzo per la conservazione estendibile di un anno. In genere consigliamo questa opzione anche per i data store di eventi che raccolgono elementi di AWS Config configurazione, prove di Audit Manager ed eventi dall'esterno AWS.

Se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni, scegli l'opzione Prezzo per la conservazione di sette anni.

Valuta l'importazione mensile del datastore di eventi nel tempo

Valuta lo storico mensile dell'importazione del datastore di eventi per verificare se esiste un'opzione di prezzo più adatta alle tue esigenze.

Se disponi di un datastore di eventi esistente con l'opzione Prezzo per la conservazione di sette anni e importi meno di 25 TB di dati al mese, valuta la possibilità di aggiornarlo e utilizzare l'opzione Prezzo per la conservazione estendibile di un anno. Per i data store di eventi che utilizzano l'opzione di conservazione dei prezzi per sette anni, è possibile modificare l'opzione di prezzo utilizzando la CloudTrail console o UpdateEventDataStoreil funzionamento dell'AWS CLIAPI.

Se disponi di un datastore di eventi esistente con l'opzione Prezzo per la conservazione estendibile di un anno e importi più di 25 TB di dati di eventi al mese, valuta se l'opzione Prezzo per la conservazione di sette anni è più in linea con le tue esigenze. Per utilizzare la nuova

opzione di prezzo, interrompi l'importazione nel datastore di eventi e crea un nuovo datastore con l'opzione Prezzo per la conservazione di sette anni.

Utilizza i selettori di eventi avanzati per filtrare gli eventi che non ti interessano

Quando si configura un Event Data Store per eventi di CloudTrail gestione, eventi di dati o eventi di attività di rete, è possibile filtrare gli eventi che non sono di interesse utilizzando selettori di eventi avanzati.

È possibile filtrare gli eventi di gestione nei seguenti campi avanzati di selezione degli eventi:`eventName`,`eventSource`, `eventTypereadOnly`, `sessionCredentialFromConsole` e. `userIdentity.arn`

È possibile filtrare gli eventi relativi ai dati nei seguenti campi avanzati di selezione degli eventi: `eventNameeventSource`,`eventType`,`resources.type`,, `resources.ARN` `readOnlysessionCredentialFromConsole`, e. `userIdentity.arn` Per ulteriori informazioni, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.

È possibile filtrare gli eventi delle attività di rete nei seguenti campi avanzati di selezione degli eventi:`eventName`,`errorCode`, e. `vpcEndpointId` Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.

Scegli un intervallo di tempo più ristretto quando copi gli eventi del percorso

Quando copi gli eventi del trail su CloudTrail Lake, specifica un'ora di inizio e un'ora di fine dell'evento più ristrette per ridurre la quantità di dati ingeriti.

Se stai copiando gli eventi del trail su CloudTrail Lake per l'analisi storica e non desideri importare eventi futuri, deseleziona l'opzione di inserimento degli eventi in modo da non incorrere in addebiti per l'importazione di eventi aggiuntivi.

Formatta le query affinché utilizzino un'**`eventTime`** di inizio e una di fine

Quando si eseguono le query in Lake, si paga in base alla quantità di dati scansionati. È possibile limitare i costi specificando un'`eventTime` di inizio e una di fine per la query.

Consulta anche

- Prezzi di AWS CloudTrail
- Metriche supportate CloudWatch
- Gestisci i costi con Budget AWS

- Nozioni di base su Esploratore dei costi

Lavorare con la cronologia CloudTrail degli eventi

CloudTrail è abilitato di default per il tuo AWS account e hai automaticamente accesso alla cronologia CloudTrail degli eventi. La cronologia degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione in un. Regione AWS Questi eventi registrano le attività svolte tramite, e. AWS Management Console AWS Command Line Interface AWS SDKs APIs La cronologia degli eventi registra gli eventi nel Regione AWS luogo in cui si è verificato l'evento. Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Puoi cercare gli eventi relativi alla creazione, alla modifica o all'eliminazione di risorse (come utenti IAM o EC2 istanze Amazon) nella tua regione per regione Account AWS sulla CloudTrail console visualizzando la pagina Cronologia eventi. Puoi cercare questi eventi anche eseguendo il comando `aws cloudtrail lookup-events` o utilizzando l'API `LookupEvents`.

Puoi utilizzare la pagina della cronologia degli eventi sulla CloudTrail console per visualizzare, cercare, scaricare, archiviare, analizzare e rispondere alle attività dell'account AWS nell'infrastruttura. Puoi personalizzare la visualizzazione della pagina della cronologia degli eventi sulla console selezionando quanti eventi visualizzare su ogni pagina e quali colonne visualizzare o nascondere. Puoi anche confrontare i dettagli degli eventi nella cronologia degli eventi side-by-side. È possibile cercare gli eventi a livello di programmazione utilizzando o. AWS SDKs AWS Command Line Interface

> **Note**
>
> Nel tempo, Servizi AWS potrebbe aggiungere altri eventi. CloudTrail registra questi eventi nella cronologia degli eventi, ma un record completo di 90 giorni delle attività che include gli eventi aggiunti non sarà disponibile fino a 90 giorni dopo l'aggiunta degli eventi.
> La cronologia degli eventi è separata da tutti i percorsi o gli archivi di dati degli eventi che crei per il tuo account. Le modifiche apportate agli archivi dati o ai percorsi degli eventi non influiscono sulla cronologia degli eventi.

Le sezioni seguenti descrivono come cercare gli eventi di gestione recenti utilizzando la CloudTrail console e il AWS CLI, e descrivono come scaricare un file di eventi. Per informazioni sull'utilizzo dell'`LookupEvents`API per recuperare informazioni dagli CloudTrail eventi, consulta LookupEventsl'AWS CloudTrail API Reference.

Argomenti

- Limitazioni della cronologia degli eventi
- Visualizzazione degli eventi di gestione recenti con la console
- Visualizzazione degli eventi gestionali recenti con AWS CLI

Limitazioni della cronologia degli eventi

Le seguenti limitazioni si applicano alla cronologia degli eventi.

- La pagina della cronologia degli eventi sulla CloudTrail console mostra solo gli eventi di gestione. Non mostra eventi relativi ai dati, eventi Insights o eventi di attività di rete.
- La cronologia degli eventi è limitata agli ultimi 90 giorni di eventi. Per una registrazione continua degli eventi nel tuo Account AWS, crea un archivio dati degli eventi o un percorso.
- Quando scarichi eventi dalla pagina Cronologia eventi sulla CloudTrail console, puoi scaricare fino a 200.000 eventi in un unico file. Se raggiungi il limite di 200.000 eventi, la CloudTrail console offrirà la possibilità di scaricare file aggiuntivi.
- La cronologia degli eventi non fornisce l'aggregazione degli eventi a livello di organizzazione. Per registrare gli eventi all'interno della tua organizzazione, crea un datastore di eventi o un percorso dell'organizzazione.
- Una ricerca nella cronologia degli eventi è limitata a un singolo evento Account AWS, restituisce solo gli eventi di un singolo Regione AWS evento e non può interrogare più attributi. Puoi applicare un solo filtro attributo e un filtro intervallo di tempo.

  Puoi creare un data store di eventi CloudTrail Lake per eseguire query su più attributi e Regioni AWS. Puoi anche eseguire query su più elementi Account AWS di un' AWS Organizations organizzazione. In CloudTrail Lake, puoi eseguire query su più tipi di eventi, inclusi eventi di gestione, eventi relativi ai dati, eventi Insights, elementi di AWS Config configurazione, evidenze di Audit Manager e non AWS eventi. CloudTrail Le query su Lake offrono una visione più approfondita e personalizzabile degli eventi rispetto alle semplici ricerche di chiavi e valori nella pagina della cronologia degli eventi o tramite esecuzione. `LookupEvents` Per ulteriori informazioni, consultare Lavorare con AWS CloudTrail Lake e Crea un archivio dati di CloudTrail eventi per gli eventi con la console.
- Non puoi escludere AWS KMS o escludere eventi Amazon RDS Data API dalla cronologia degli eventi; le impostazioni che applichi a un trail o a un event data store non si applicano alla cronologia degli eventi.

Visualizzazione degli eventi di gestione recenti con la console

È possibile utilizzare la pagina Cronologia degli eventi nella CloudTrail console per visualizzare gli ultimi 90 giorni di eventi di gestione in un file Regione AWS. Puoi anche scaricare un file contenente queste informazioni o a un sottoinsieme di informazioni in base al filtro e all'intervallo di tempo scelti. È possibile personalizzare la visualizzazione della cronologia degli eventi selezionando il numero di eventi da visualizzare su ciascuna pagina e scegliendo quali colonne visualizzare sulla console. È inoltre possibile cercare e filtrare eventi in base ai tipi di risorse disponibili per un determinato servizio. Puoi selezionare fino a cinque eventi nella cronologia degli eventi e confrontarne i dettagli side-by-side.

Event history (Cronologia eventi) non visualizza gli eventi di dati. Per visualizzare gli eventi di dati, crea un datastore di eventi o un percorso.

Dopo 90 giorni, gli eventi non vengono più visualizzati nella cronologia degli eventi. Non è possibile eliminare manualmente gli eventi dalla cronologia degli eventi.

Per ulteriori informazioni sulle modalità di CloudTrail registrazione degli eventi per un servizio specifico, è possibile consultare la documentazione relativa a tale servizio. Per ulteriori informazioni, consulta AWS argomenti di servizio per CloudTrail.

> **Note**
>
> Per una registrazione continua delle attività e degli eventi degli ultimi 90 giorni, crea un archivio dati sugli eventi o un percorso.

Visualizzazione della Cronologia degli eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi). Consultare un elenco filtrato di eventi, con gli eventi più recenti visualizzati per primi. Il filtro predefinito per gli eventi è di Read-only (Sola lettura), impostato su false (Falso). È possibile rimuovere il filtro scegliendo la X alla sua destra.
3. Puoi filtrare gli eventi in base a un singolo attributo, che puoi scegliere dall'elenco a discesa. Per filtrare in base a un attributo, scegli l'attributo dall'elenco a discesa e inserisci il valore completo dell'attributo. Ad esempio, per visualizzare tutti gli eventi di accesso alla console, scegli il filtro

Nome evento e specifica. ConsoleLogin Oppure, per visualizzare gli eventi di gestione di S3 recenti, scegli il filtro di origine degli eventi e specifica`s3.amazonaws.com`.

4. Per visualizzare un evento di gestione specifico, scegli il nome dell'evento. Nella pagina dei dettagli dell'evento, è possibile visualizzare i dettagli dell'evento, visualizzare le risorse di riferimento e visualizzare il record dell'evento.
5. Per confrontare gli eventi, seleziona fino a cinque eventi compilando le relative caselle di controllo sul margine sinistro della tabella Event history (Cronologia eventi). Puoi visualizzare i dettagli degli eventi selezionati side-by-side nella tabella Confronta i dettagli degli eventi.
6. È possibile salvare la cronologia eventi scaricandola come file in formato JSON o CSV. Il download della cronologia eventi può richiedere alcuni minuti.

Indice

- Navigazione tra le pagine
- Personalizzazione dello schermo
- Filtraggio degli eventi CloudTrail
- Visualizzazione dei dettagli per un evento
- Download di eventi
- Visualizzazione di risorse a cui viene fatto riferimento tramite AWS Config

Navigazione tra le pagine

Puoi navigare tra le pagine della Cronologia degli eventi scegliendo la pagina che desideri visualizzare. Puoi anche visualizzare la pagina successiva e precedente nella Cronologia degli eventi.

Scegli **<** per visualizzare la pagina precedente della Cronologia degli eventi.

Scegli **>** per visualizzare la pagina successiva della Cronologia degli eventi.

Personalizzazione dello schermo

È possibile personalizzare la visualizzazione della cronologia degli eventi sulla CloudTrail console selezionando una delle seguenti preferenze.

- Dimensioni della pagina: scegli se visualizzare 10, 25 o 50 eventi su ogni pagina.

- Righe a capo: avvolgi il testo in modo da poter vedere tutto il testo per ogni evento.
- Righe a strisce: ombreggia ogni altra riga nella tabella.
- Visualizzazione dell'ora dell'evento: scegli se visualizzare l'ora dell'evento in UTC o nel fuso orario locale.
- Seleziona colonne visibili: seleziona le colonne che desideri visualizzare. Per impostazione di default, vengono visualizzate le seguenti colonne:
  - Nome evento
  - Event time (Ora evento)
  - Nome utente
  - Origine eventi
  - Tipo di risorsa
  - Nome risorsa

> **Note**
>
> Non puoi modificare l'ordine delle colonne o eliminare manualmente gli eventi da Event history (Cronologia eventi).

Personalizzazione dello schermo

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
3. Scegliere l'icona a forma di ingranaggio.
4. Per Dimensioni della pagina, scegli il numero di eventi da visualizzare su una pagina.
5. Scegli Righe a capo per vedere tutto il testo di ogni evento.
6. Scegli Righe a strisce per ombreggiare ogni altra riga nella tabella.
7. Per Visualizzazione dell'ora dell'evento scegli se visualizzare l'ora dell'evento in UTC o nel fuso orario locale. Per impostazione predefinita, è selezionato UTC.
8. In Select visible columns (Seleziona colonne visibili), seleziona le colonne che desideri visualizzare. Disattiva le colonne che non desideri visualizzare.
9. Una volta apportate le modifiche, scegli Conferma.

Filtraggio degli eventi CloudTrail

La visualizzazione predefinita degli eventi nella cronologia di eventi utilizza un attributo filtro per escludere gli eventi di sola lettura dall'elenco di eventi visualizzati. Questo filtro attributo è denominato Read-only (Sola lettura) ed è impostato su false. Puoi rimuovere questo filtro per visualizzare gli eventi in lettura e in scrittura. Per visualizzare solo gli eventi Read (Lettura), puoi modificare il valore del filtro impostandolo su true. Puoi filtrare gli eventi anche in base ad altri attributi. Puoi inoltre filtrare in base all'intervallo di tempo.

> **Note**
>
> Puoi applicare un solo filtro attributo e un filtro intervallo di tempo. Non è possibile applicare più filtri attributo.

AWS chiave di accesso

L'ID della chiave di AWS accesso utilizzata per firmare la richiesta. Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, corrisponde all'ID della chiave di accesso delle credenziali temporanee.

ID evento

L' CloudTrail ID dell'evento. Ogni evento ha un ID univoco.

Nome evento

Nome dell'evento. Ad esempio, puoi filtrare gli eventi IAM, ad esempio`CreatePolicy`, o EC2 gli eventi Amazon, come`RunInstances`.

Origine eventi

Il AWS servizio a cui è stata effettuata la richiesta, ad esempio `iam.amazonaws.com` `os3.amazonaws.com`. È possibile scorrere un elenco di origini degli eventi dopo aver scelto il filtro Event source (Origine eventi).

Sola lettura

Tipo di evento di lettura. Gli eventi sono classificati come eventi di lettura o scrittura. Se è impostato su false, gli eventi di lettura non sono inclusi nell'elenco degli eventi visualizzati. Per impostazione predefinita, questo filtro attributo viene applicato con il valore false.

Nome risorsa

Nome o ID della risorsa a cui l'evento fa riferimento. Ad esempio, il nome della risorsa potrebbe essere "auto-scaling-test-group" per un gruppo Auto Scaling o «i-12345678910" per un'istanza. EC2

Tipo di risorsa

Tipo della risorsa a cui l'evento fa riferimento. Ad esempio, un tipo di risorsa può essere per o per RDS. `Instance` EC2 `DBInstance` I tipi di risorse variano per ogni AWS servizio.

Intervallo temporale

Intervallo di tempo in cui si desidera filtrare gli eventi. Puoi scegliere un Intervallo relativo o un Intervallo assoluto. È possibile filtrare gli eventi per gli ultimi 90 giorni.

Nome utente

L'identità a cui l'evento fa riferimento. Ad esempio, può essere un utente, il nome di un ruolo o un ruolo del servizio.

Se non sono presenti eventi registrati per l'attributo o l'intervallo di tempo scelto, l'elenco dei risultati è vuoto. È possibile applicare solo un filtro attributo oltre all'intervallo di tempo. Se si scegli un filtro attributo diverso, l'intervallo di tempo specificato viene conservato.

La procedura riportata di seguito illustra come filtrare i dati in base a un attributo.

Per filtrare in base un attributo

1. Per filtrare i risultati in base a un attributo, scegli un attributo dall'elenco a discesa Lookup attributes (Attributi di ricerca) e quindi digita o scegli un valore per l'attributo nella casella di testo.
2. Per rimuovere un filtro attributo, scegli X a destra della casella del filtro attributo.

La procedura riportata di seguito illustra come filtrare in base alla data e all'ora di inizio e fine.

Per filtrare in base a una data e ora di inizio e fine

1. Per restringere l'intervallo di tempo relativo agli eventi che desideri visualizzare, scegli un intervallo di tempo nella barra dell'intervallo di tempo. Puoi scegliere un Intervallo relativo o un Intervallo assoluto.

Scegli Intervallo relativo per selezionare un intervallo di tempo predefinito o un intervallo personalizzato. I valori preimpostati sono 30 minuti, 1 ora, 12 ore o 1 giorno. Per specificare un intervallo di tempo personalizzato, scegli Custom (Personalizzato).

Scegli Intervallo assoluto per specificare un'ora di inizio e di fine specifica. Inoltre, è possibile scegliere tra UTC e fuso orario locale.

2. Per rimuovere un filtro dell'intervallo di tempo, scegli Cancella sulla barra dell'intervallo di tempo.

Visualizzazione dei dettagli per un evento

1. Scegliere un evento nell'elenco dei risultati per visualizzare i relativi dettagli.
2. Le risorse a cui si fa riferimento nell'evento sono mostrate nella tabella Resources referenced (Risorse di riferimento) nella pagina dei dettagli dell'evento.
3. Alcune risorse di riferimento sono associate a collegamenti. Scegliere il collegamento per aprire la console per la risorsa corrispondente.
4. Scorri fino a Event record (Record di eventi) nella pagina dei dettagli per visualizzare il record degli eventi JSON, chiamato anche payload dell'evento.
5. Scegli Event history (Cronologia eventi) nel percorso di navigazione della pagina per chiudere la pagina dei dettagli dell'evento e tornare a Event history (Cronologia eventi).

Download di eventi

È possibile scaricare la cronologia degli eventi registrati come file in formato JSON o CSV. Puoi scaricare fino a 200.000 eventi in un unico file. Se raggiungi il limite di 200.000 eventi, la CloudTrail console offrirà la possibilità di scaricare file aggiuntivi. Utilizzare i filtri e gli intervalli di tempo per ridurre le dimensioni del file scaricato.

> **Note**
>
> CloudTrail i file di cronologia degli eventi sono file di dati che contengono informazioni (come i nomi delle risorse) che possono essere configurate dai singoli utenti. Alcuni dati potrebbero essere interpretati come comandi nei programmi utilizzati per leggere e analizzare questo tipo di informazioni (rischio di attacco di tipo CSV Injection o Formula Injection). Ad esempio, quando CloudTrail gli eventi vengono esportati in formato CSV e importati in un programma per fogli di calcolo, tale programma potrebbe avvisare l'utente in merito a

problemi di sicurezza. È consigliabile scegliere di disabilitare questi contenuti per proteggere il sistema. Disabilitare sempre i collegamenti o le macro nei file della cronologia degli eventi scaricati.

1. Aggiungi un filtro e un intervallo di tempo per gli eventi in Event history (Cronologia eventi) che desideri scaricare. Ad esempio, è possibile specificare il nome dell'evento, `StartInstances`, e specificare un intervallo di tempo per gli ultimi tre giorni di attività.
2. Seleziona Download events (Download di eventi), quindi Download as CSV (Scarica in formato CSV) o Download as JSON (Scarica in formato JSON). Il download inizierà immediatamente.

   > **Note**
   >
   > Il download potrebbe richiedere alcuni minuti per il completamento. Per ottenere più rapidamente i risultati, prima di avviare il processo di download, utilizzare un filtro più specifico o un intervallo di tempo più breve per limitare i risultati. Puoi annullare un download. Se annulli un download, è possibile che nel computer locale sia presente un download parziale che include solo alcuni dati relativi agli eventi. Per scaricare la cronologia completa degli eventi, riavvia il download.

3. Al termine del download, aprire il file per visualizzare gli eventi specificati.
4. Per annullare il download, scegli Cancel (Annulla) e quindi conferma scegliendo Cancel download (Annulla download). Se devi riavviare un download, attendi che l'annullamento del download precedente sia terminato.

Visualizzazione di risorse a cui viene fatto riferimento tramite AWS Config

AWS Config registra i dettagli di configurazione, le relazioni e le modifiche alle risorse. AWS

Nel riquadro Risorse a cui si fa riferimento, scegli

nella colonna della cronologia AWS Config delle risorse per visualizzare la risorsa nella console. AWS Config

Se
l' icona
è grigia, AWS Config non è attivata o non registra il tipo di risorsa. Scegli l'icona per accedere alla

AWS Config console e attivare il servizio o iniziare a registrare quel tipo di risorsa. Per ulteriori informazioni, consulta Configurazione AWS Config tramite la console nella Guida per gli AWS Config sviluppatori.

Se nella colonna viene visualizzato il messaggio Link not available (Collegamento non disponibile), la risorsa non può essere visualizzata per uno dei seguenti motivi:

- AWS Config non supporta il tipo di risorsa. Per ulteriori informazioni, consulta Risorse supportate, elementi di configurazione e relazioni nella Guida per gli sviluppatori di AWS Config .
- AWS Config recentemente ha aggiunto il supporto per il tipo di risorsa, ma non è ancora disponibile nella CloudTrail console. Puoi cercare la risorsa nella AWS Config console per vedere la sequenza temporale della risorsa.
- La risorsa è di proprietà di un altro Account AWS.
- La risorsa è di proprietà di un altro Servizio AWS, ad esempio una policy IAM gestita.
- La risorsa è stata creata e quindi eliminata immediatamente.
- La risorsa è stata creata o aggiornata di recente.

Per concedere agli utenti l'autorizzazione di sola lettura per visualizzare le risorse nella AWS Config console, consulta. Concessione dell'autorizzazione alla visualizzazione delle AWS Config informazioni sulla console CloudTrail

Per ulteriori informazioni in merito AWS Config, consulta la Guida per gli AWS Config sviluppatori.

Visualizzazione degli eventi gestionali recenti con AWS CLI

È possibile cercare gli eventi di CloudTrail gestione degli ultimi 90 giorni per quelli correnti Regione AWS utilizzando il aws cloudtrail lookup-events comando. Il aws cloudtrail lookup-events comando mostra gli eventi nel Regione AWS luogo in cui si sono verificati.

La ricerca supporta i seguenti attributi per gli eventi di gestione:

- AWS chiave di accesso
- ID evento
- Nome evento
- Origine eventi

- Sola lettura
- Nome risorsa
- Tipo di risorsa
- Nome utente

Tutti gli attributi sono facoltativi.

Il comando `lookup-events` include le seguenti opzioni:

- `--max-items` *`<integer>`*— Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili supera il valore specificato, viene fornito un `NextToken` nell'output del comando. Per riprendere la paginazione, specifica il valore di `NextToken` nell'argomento starting-token di un comando successivo. Non utilizzare l'elemento di risposta `NextToken` direttamente al di fuori della AWS CLI.
- `--start-time` *`<timestamp>`*— specifica che vengono restituiti solo gli eventi che si verificano dopo o all'ora specificata. Se l'ora di inizio specificata è successiva all'ora di fine specificata, viene restituito un errore.
- `--lookup-attributes` *`<integer>`*— Contiene un elenco di attributi di ricerca. Al momento, l'elenco può contenere solo un elemento.
- `--generate-cli-skeleton` *`<string>`*— Stampa uno scheletro JSON sullo standard output senza inviare una richiesta API. Se fornito senza alcun valore o senza l'input, stampa un JSON di input di esempio che può essere utilizzato come argomento per `--cli-input-json`. Allo stesso modo, se viene fornito yaml-input, stamperà un input YAML di esempio con cui è possibile utilizzare `--cli-input-yaml`. Se fornito con l'output del valore, convalida gli input del comando e restituisce un esempio di output JSON per quel comando. Lo scheletro JSON generato non è stabile tra le versioni di AWS CLI e non vi sono garanzie di compatibilità con le versioni precedenti nello scheletro JSON generato.
- `--cli-input-json` *`<string>`*— Legge gli argomenti dalla stringa JSON fornita. La stringa JSON segue il formato fornito dal parametro `--generate-cli-skeleton`. Se vengono forniti altri argomenti sulla riga di comando, tali valori sostituiranno i valori forniti da JSON. Non è possibile passare valori binari arbitrari utilizzando un valore fornito da JSON poiché la stringa verrà presa alla lettera. Questo non può essere specificato insieme al parametro `--cli-input-yaml`.

Per informazioni generali sull'uso dell'interfaccia a riga di AWS comando, consulta la Guida per l'AWS Command Line Interface utente.

Indice

- Prerequisiti
- Visualizzazione delle informazioni di aiuto della riga di comando
- Ricerca di eventi
- Specifica del numero di eventi da restituire
- Ricerca di eventi in base a un intervallo di tempo
- Ricerca di eventi in base a un attributo
  - Esempi di ricerca in base a un attributo
- Specifica della pagina di risultati successiva
- Recupero dell'input JSON da un file
- Campi di output della ricerca

Prerequisiti

- Per eseguire AWS CLI i comandi, è necessario installare AWS CLI. Per informazioni, consulta la Guida introduttiva a AWS CLI.
- Assicurati che la tua AWS CLI versione sia successiva alla 1.6.6. Per verificare la versione della CLI, esegui aws --version nella riga di comando.
- Per impostare l'account e il Regione AWS formato di output predefinito per una AWS CLI sessione, usa il aws configure comando. Per ulteriori informazioni, vedere Configurazione dell'interfaccia a riga di AWS comando.

> **Note**
>
> I CloudTrail AWS CLI comandi fanno distinzione tra maiuscole e minuscole.

Visualizzazione delle informazioni di aiuto della riga di comando

Per visualizzare le informazioni di aiuto della riga di comando per `lookup-events`, digita il comando seguente:

```
aws cloudtrail lookup-events help
```

Ricerca di eventi

> **Important**
>
> La frequenza delle richieste di ricerca è limitata a due al secondo, per account, per Regione. Se questo limite viene superato, si verifica un errore di limitazione.

Per visualizzare i dieci eventi più recenti, digita il comando seguente:

```
aws cloudtrail lookup-events --max-items 10
```

Un evento restituito è simile al seguente esempio fittizio, che è stato formattato per agevolarne la lettura:


```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
```

```
                    \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                    \"eventType\":\"AwsApiCall\",
                    \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

Per una spiegazione dei campi correlati alla ricerca nell'output, vedere la sezione Campi di output della ricerca più avanti in questo documento. Per una spiegazione dei campi dell' CloudTrail evento, vedere. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete

Specifica del numero di eventi da restituire

Per specificare il numero di eventi da restituire, digita il comando seguente:

```
aws cloudtrail lookup-events --max-items <integer>
```

I valori possibili sono da 1 a 50. L'esempio seguente restituisce un evento.

```
aws cloudtrail lookup-events --max-items 1
```

Ricerca di eventi in base a un intervallo di tempo

Gli eventi negli ultimi 90 giorni sono disponibili per la ricerca. Per specificare un intervallo di tempo, digita il comando seguente:

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *`<timestamp>`* specifica, in UTC, che vengano restituiti solo gli eventi che si sono verificati in corrispondenza o dopo l'intervallo di tempo specificato. Se l'ora di inizio specificata è successiva all'ora di fine specificata, viene restituito un errore.

`--end-time` *`<timestamp>`* specifica, in UTC, che vengano restituiti solo gli eventi che si sono verificati in corrispondenza o prima dell'intervallo di tempo specificato. Se l'ora di fine specificata è anteriore all'ora di inizio specificata, viene restituito un errore.

L'ora di inizio di default è la prima data in cui i dati sono disponibili negli ultimi 90 giorni. L'ora di fine di default è invece l'ora dell'evento che si è verificato più in vicinanza dell'ora corrente.

Tutti i timestamp sono mostrati in UTC.

Ricerca di eventi in base a un attributo

Per filtrare in base a un attributo, digita il comando seguente:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Puoi specificare solo una coppia chiave/valore attributo per ogni comando lookup-events. Di seguito sono riportati i valori validi per `AttributeKey`. I nomi dei valori fanno distinzione tra lettere maiuscole e minuscole.

- `AccessKeyId`
- `EventId`
- `EventName`
- `EventSource`
- `ReadOnly`
- `ResourceName`
- `ResourceType`
- `Username`

La lunghezza massima per `AttributeValue` è di 2000 caratteri. I seguenti caratteri ('_', ' ', ',', '\ \n') contano come due caratteri nel limite di 2000 caratteri.

Esempi di ricerca in base a un attributo

Il comando di esempio seguente restituisce gli eventi in cui il valore di `AccessKeyId` è `AKIAIOSFODNN7EXAMPLE`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

Il comando di esempio seguente restituisce l'evento per il valore CloudTrail `EventId` specificato.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Il comando di esempio seguente restituisce gli eventi in cui il valore di `EventName` è `RunInstances`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

Il comando di esempio seguente restituisce gli eventi in cui il valore di `EventSource` è `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

Il comando di esempio seguente restituisce gli eventi di scrittura. Esclude gli eventi di lettura, ad esempio `GetBucketLocation` e `DescribeStream`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

Il comando di esempio seguente restituisce gli eventi in cui il valore di `ResourceName` è `CloudTrail_CloudWatchLogs_Role`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

Il comando di esempio seguente restituisce gli eventi in cui il valore di `ResourceType` è `AWS::S3::Bucket`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

Il comando di esempio seguente restituisce gli eventi in cui il valore di `Username` è `root`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Specifica della pagina di risultati successiva

Per visualizzare la pagina di risultati successiva mediante un comando `lookup-events`, digita il comando seguente:

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

dove il valore di `<token>` è preso dal primo campo dell'output del comando precedente.

Quando utilizzi `--next-token` in un comando, devi utilizzare gli stessi parametri usati nel comando precedente. Ad esempio, supponiamo che tu abbia eseguito il seguente configurazione:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Per visualizzare la pagina di risultati successiva, il comando successivo avrà il formato seguente:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

Recupero dell'input JSON da un file

AWS CLI Per alcuni AWS servizi sono disponibili due parametri, `--generate-cli-skeleton` uno dei quali è possibile utilizzare per generare un modello JSON che è possibile modificare e utilizzare come input per il `--cli-input-json` parametro. `--cli-input-json` Questa sezione descrive come utilizzare questi parametri con `aws cloudtrail lookup-events`. Per informazioni più generali, consulta AWS CLI scheletri e file di input.

Per cercare CloudTrail gli eventi ottenendo l'input JSON da un file

1. Crea un modello di input da usare con `lookup-events` reindirizzando l'output di `--generate-cli-skeleton` in un file, come nell'esempio seguente.

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   Il file modello generato (in questo caso, LookupEvents .txt) ha il seguente aspetto:

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
   ```

```
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Utilizza un editor di testo per modificare l'input JSON in base alle esigenze. L'input JSON deve contenere solo i valori specificati.

> **Important**
>
> Tutti i valori vuoti o null devono essere rimossi dal modello prima di utilizzarlo.

L'esempio seguente specifica un intervallo di tempo e il numero massimo di risultati da restituire.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Per utilizzare il file modificato come input, utilizzate la sintassi `--cli-input-json file://<filename>`, come nell'esempio seguente:

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> Puoi usare altri argomenti sulla stessa riga di comando come `--cli-input-json`.

Campi di output della ricerca

Eventi

Un elenco di eventi di ricerca in base all'attributo di ricerca e all'intervallo di tempo specificati. L'elenco di eventi è ordinato in base all'ora, con l'ultimo evento elencato per primo. Ogni voce

contiene informazioni sulla richiesta di ricerca e include una rappresentazione in formato stringa dell' CloudTrail evento recuperato.

Le voci seguenti descrivono i campi in ogni evento di ricerca.

CloudTrailEvent

Stringa JSON contenente una rappresentazione oggetto dell'evento restituito. Per informazioni su ciascuno degli elementi restituiti, consulta l'argomento relativo al contenuto del corpo dei record.

EventId

Stringa contenente il GUID dell'evento restituito.

EventName

Stringa contenente il nome dell'evento restituito.

EventSource

Il AWS servizio a cui è stata inoltrata la richiesta.

EventTime

Data e ora, in formato UNIX, dell'evento.

Risorse

Elenco delle risorse a cui fa riferimento l'evento restituito. Ogni voce specifica un tipo e un nome di risorsa.

ResourceName

Stringa contenente il nome della risorsa a cui l'evento fa riferimento.

ResourceType

Stringa contenente il tipo di una risorsa a cui l'evento fa riferimento. Quando risulta impossibile determinare il tipo di risorsa, viene restituito un valore null.

Nome utente

Stringa contenente il nome utente dell'account per l'evento restituito.

NextToken

Stringa per visualizzare la pagina di risultati successiva generata da un precedente comando `lookup-events`. Per usare il token, i parametri devono essere uguali a quelli specificati nel

comando originale. Se nell'output non è presente alcuna voce `NextToken`, significa che non sono presenti altri risultati da restituire.

Lavorare con CloudTrail Insights

AWS CloudTrail Insights aiuta AWS gli utenti a identificare e rispondere alle attività insolite associate ai tassi di chiamata e ai tassi di errore delle API analizzando continuamente gli eventi di CloudTrail gestione. CloudTrail Insights analizza gli eventi di gestione passati per stabilire i normali modelli di frequenza delle chiamate e dei tassi di errore delle API, noti anche come baseline. CloudTrail genera quindi eventi Insights quando i tassi di chiamata API o i tassi di errore correnti si discostano dalla linea di base.

Puoi raccogliere due tipi di Insights:

- Frequenza di chiamata API: misurazione delle chiamate API di gestione in sola scrittura che si verificano al minuto rispetto a un volume di chiamate API di base. Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il trail o event data store deve abilitare Insights e registrare `write` gli eventi di gestione.
- Tasso di errore delle API: una misurazione delle chiamate API di gestione che generano codici di errore. L'errore viene visualizzato se la chiamata API non ha esito positivo. Per registrare gli eventi di Insights sul tasso di errore dell'API, il trail o event data store deve abilitare Insights e registrare gli eventi `read` o la `write` gestione oppure entrambi `read` gli eventi di `write` gestione.

CloudTrail Insights analizza gli eventi di gestione che si verificano in ogni regione per il trail o event data store e genera un evento Insights quando viene rilevata un'attività insolita che si discosta dalla linea di base. Un evento CloudTrail Insights viene generato nella stessa regione in cui viene generato l'evento di gestione di supporto.

Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Argomenti

- Costi per gli eventi Insights
- Erogazione di eventi Insights
- Registrazione degli eventi di Insights con la console CloudTrail
- Registrazione degli eventi di Insights con AWS CLI
- Visualizzazione di eventi Insights per i percorsi
- Visualizzazione degli eventi Insights per i datastore di eventi

Costi per gli eventi Insights

Quando abiliti gli eventi Insights su un trail o event data store esistente, CloudTrail analizza gli ultimi 28 giorni di eventi di gestione raccolti dal trail o event data store per stabilire una linea di base della normale attività. Dopo la creazione della baseline iniziale, la baseline viene ricalcolata ogni giorno sugli ultimi 28 giorni di dati. Non sono CloudTrail previsti costi per l'analisi di base.

Dopo l'analisi di base, ti verranno addebitati gli CloudTrail addebiti per eventuali eventi gestionali futuri analizzati da. CloudTrail Vengono addebitati addebiti in base al numero di eventi di gestione analizzati per i tipi di Insights abilitati.

Se scegli di registrare entrambi i tipi di Insights per un data store o un data store di eventi che registra `read` e `write` gestisce gli eventi, il numero totale di eventi analizzati sarà maggiore del numero totale di eventi di gestione registrati. Questo perché CloudTrail analizzerà gli eventi di gestione in sola scrittura due volte, una volta per calcolare la frequenza delle chiamate API e un'altra per determinare il tasso di errore dell'API. Gli eventi di gestione in sola lettura verranno analizzati una volta per calcolare il tasso di errore dell'API.

Puoi identificare gli addebiti per gli eventi Insights sulla tua fattura cercando il tipo di `InsightsEvents` utilizzo. Per ulteriori informazioni, consulta Visualizzazione dei CloudTrail costi e dell'utilizzo con AWS Cost Explorer.

Con Insights abilitato, ti verranno addebitati addebiti per eventi Insights separati per ogni archivio dati di percorsi ed eventi. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS CloudTrail.

Esempio 1: abilita Insights per la frequenza delle chiamate API e il tasso di errore delle API su un percorso

In questo primo esempio, abiliti Insights su un trail e scegli di raccogliere entrambi i tipi di Insights. Il percorso in questo esempio registra sia gli eventi di gestione che quelli `read` di `write` gestione.

- CloudTrail analizza gli eventi di gestione registrati negli ultimi 28 giorni per formare una linea di base. Non sono CloudTrail previsti costi per l'analisi.
- Dopo la creazione della baseline, il trail registra 300.000 eventi di gestione, di cui 270.000 eventi di gestione e 30.000 eventi di `read` gestione. `write`
  - Gli eventi di `write` gestione vengono analizzati due volte, una volta per la frequenza delle chiamate API e una volta per il tasso di errore dell'API (30.000* 2=60.000).
  - Gli eventi di `read` gestione vengono analizzati una volta per determinare il tasso di errore dell'API (270.000*1=270.000).

- Gli eventi di gestione totali analizzati sono 330.000 (60.000 + 270.000). Dovrai sostenere i costi per l'analisi di 330.000 eventi di gestione per questo percorso. Ti verrà addebitato separatamente se abiliti Insights per un altro percorso o un data store di eventi.

Esempio 2: abilitare Insights per due percorsi

Nel prossimo esempio, si abilita Insights su due percorsi, trail A e trail B. Si sceglie di abilitare API call rate Insights solo sul trail A e API error rate Insights solo sul trail B. Entrambi i trail registrano `read` e `write` gestiscono gli eventi.

- CloudTrail analizza gli eventi di `write` gestione registrati negli ultimi 28 giorni per formare una linea di base. Non sono CloudTrail previsti costi per l'analisi.
- Dopo la creazione della baseline, i trail registrano 800.000 eventi di gestione, di cui 710.000 `read` eventi e 90.000 eventi. `write`

  Per il percorso A, viene eseguita la seguente analisi:

  - Gli eventi `write` di gestione vengono analizzati una sola volta per determinare la frequenza delle chiamate API (90.000 * 1=90.000).
  - Gli eventi `read` di gestione non vengono analizzati, poiché analizza CloudTrail solo gli eventi di `write` gestione per API Call rate Insights.
  - Il totale degli eventi di gestione analizzati è di 90.000. Saranno sostenuti i costi per l'analisi di 90.000 eventi di gestione per il percorso A.

  Per la traccia B, viene eseguita la seguente analisi:

  - Gli eventi `write` di gestione vengono analizzati una sola volta per determinare il tasso di errore dell'API (90.000 * 1=90.000).
  - Gli eventi di `read` gestione vengono analizzati una sola volta per determinare il tasso di errore dell'API (710.000 *1=710.000).
  - Gli eventi di gestione totali analizzati sono 800.000 (90.000 + 710.000). Saranno sostenuti i costi per l'analisi di 800.000 eventi di gestione per il trail B.

Esempio 3: abilitare Insights per la frequenza delle chiamate API e il tasso di errore delle API su un trail e un data store di eventi

In questo ultimo esempio, abiliti Insights for API call rate e API error rate sia su un trail che su un event data store. Sia l'archivio dati del percorso che quello degli eventi registrano `read` e

`write` gestiscono gli eventi. Se hai abilitato CloudTrail Insights su entrambi, ti verranno addebitati separatamente i costi per Insights per il trail e l'event data store.

- CloudTrail analizza gli eventi di gestione registrati negli ultimi 28 giorni per formare una linea di base. Non sono CloudTrail previsti costi per l'analisi.
- Dopo la creazione della baseline, il trail and event data store registra 500.000 eventi di gestione, di cui 380.000 sono eventi di `read` gestione e 120.000 sono eventi di gestione. `write`

  Per il trail, viene eseguita la seguente analisi:

  - Gli eventi di `write` gestione vengono analizzati due volte per il percorso, una volta per la frequenza delle chiamate API e una volta per il tasso di errore dell'API (120.000* 2=240.000).
  - Gli eventi `read` di gestione vengono analizzati una sola volta per determinare il tasso di errore dell'API (380.000 *1=380.000).
  - Il totale degli eventi di gestione analizzati per il percorso è di 620.000 (240.000 + 380.000). Saranno sostenuti i costi per l'analisi di 620.000 eventi di gestione del percorso.

  Per l'archivio dati degli eventi, viene eseguita la seguente analisi:

  - Gli eventi di `write` gestione vengono analizzati due volte per l'Event Data Store, una volta per la frequenza delle chiamate API e una volta per il tasso di errore dell'API (120.000* 2=240.000).
  - Gli eventi di `read` gestione vengono analizzati una volta per l'Event Data Store per il tasso di errore dell'API (380.000 *1=380.000).
  - Il totale degli eventi di gestione analizzati per l'Event Data Store è di 620.000 (240.000 + 380.000). Saranno sostenuti i costi per l'analisi di 620.000 eventi di gestione per l'Event Data Store.

Erogazione di eventi Insights

A differenza di altri tipi di eventi CloudTrail acquisiti, gli eventi di Insights vengono registrati solo quando CloudTrail rilevano cambiamenti nell'utilizzo dell'API dell'account che differiscono significativamente dai modelli di utilizzo tipici dell'account.

CloudTrail Il luogo in cui vengono distribuiti gli eventi e il tempo necessario per riceverli variano a seconda dei percorsi e degli archivi di dati sugli eventi.

Distribuzione di eventi Insights per i percorsi

Se hai abilitato gli eventi di Insights su un percorso e CloudTrail rilevi attività insolite, CloudTrail invia gli eventi di Insights nella `/CloudTrail-Insight` cartella nel bucket S3 di destinazione scelto per il percorso. Dopo aver abilitato CloudTrail Insights per la prima volta su un percorso, CloudTrail potrebbero essere necessarie fino a 36 ore per iniziare a fornire gli eventi Insights, a condizione che venga rilevata un'attività insolita durante quel periodo.

Se disattivi la registrazione degli eventi di Insights su un percorso e poi riattivi gli eventi di Insights oppure interrompi e riavvii la registrazione su un percorso, possono essere necessarie fino a 36 ore per riavviare la consegna degli eventi di Insights, CloudTrail a condizione che durante quel periodo venga rilevata un'attività insolita.

Distribuzione di eventi Insights per i datastore di eventi

Se hai abilitato gli eventi Insights su un data store di eventi di origine, CloudTrail invia gli eventi di Insights al data store degli eventi di destinazione. Dopo aver abilitato CloudTrail Insights per la prima volta nell'archivio dati degli eventi di origine, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a distribuire gli eventi di Insights al data store degli eventi di destinazione, a condizione che venga rilevata un'attività insolita durante quel periodo.

Se disattivi la registrazione degli eventi di Insights su un data store di eventi di origine e quindi riattivi gli eventi di Insights o interrompi e riavvii l'inserimento degli eventi su un data store di eventi di origine, possono essere necessari fino a 7 giorni per riavviare la consegna degli eventi di Insights, CloudTrail a condizione che durante quel periodo venga rilevata un'attività insolita. Si applicano costi aggiuntivi per l'acquisizione di eventi Insights in Lake. CloudTrail Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Registrazione degli eventi di Insights con la console CloudTrail

Questa sezione descrive come abilitare gli eventi Insights su un trail o un data store di eventi esistente utilizzando la CloudTrail console.

Per ulteriori informazioni su come creare un nuovo percorso per registrare gli eventi di Insights, consultaCreazione di un percorso con la console.

Per ulteriori informazioni su come creare un nuovo archivio dati di eventi per raccogliere gli eventi di Insights, consultaCrea un archivio dati sugli eventi per gli eventi Insights con la console.

Argomenti

- Abilitare CloudTrail Insights su un percorso esistente con la console
- Abilitazione di CloudTrail Insights su un data store di eventi esistente con la console

Abilitare CloudTrail Insights su un percorso esistente con la console

Utilizzare la procedura seguente per abilitare CloudTrail Insights su un percorso esistente.

1. Nel riquadro di navigazione a sinistra della CloudTrail console, apri la pagina Trails e scegli il nome di un percorso.
2. Negli eventi Insights, scegli Modifica.

> **Note**
>
> Per la registrazione degli eventi Insights vengono applicati costi aggiuntivi. Per CloudTrail i prezzi, consulta AWS CloudTrail Prezzi.

3. In Event type (Tipo di evento), scegli Insights events (Eventi Insights).
4. In Insights events (Informazioni dettagliate eventi), in Choose Insights types (Scegli i tipi di informazioni dettagliate), scegli API call rate (Tasso di chiamata API), Tasso di errore API o entrambi. Il percorso deve registrare gli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Il percorso deve registrare gli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.
5. Per salvare le modifiche, scegliere Salva modifiche.

CloudTrail potrebbero essere necessarie fino a 36 ore per iniziare a fornire gli eventi di Insights dopo aver abilitato gli eventi Insights su una traccia, a condizione che venga rilevata un'attività insolita durante quel periodo.

Abilitazione di CloudTrail Insights su un data store di eventi esistente con la console

Utilizzare la procedura seguente per abilitare CloudTrail Insights su un data store di eventi esistente.

Si applicano costi aggiuntivi per l'acquisizione di eventi Insights in CloudTrail Lake. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

> **Note**
>
> È possibile abilitare CloudTrail Insights solo negli archivi di dati di eventi contenenti eventi di CloudTrail gestione. Non è possibile abilitare CloudTrail Insights su altri tipi di data store di eventi.

1. Nel riquadro di navigazione a sinistra della CloudTrail console, sotto Lake, scegli Event data store.
2. Scegli l'evento dal datastore di eventi.
3. Per Eventi di gestione, scegli Modifica.
4. Scegli Abilita l'acquisizione degli eventi di Insights.
5. Scegli l'event store di destinazione che raccoglierà gli eventi Insights. Il datastore di eventi di destinazione raccoglierà gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi. Per informazioni su come creare il datastore di eventi di destinazione, consulta Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights.
6. Scegli i tipi di Insights. Puoi scegliere la frequenza delle chiamate API, la frequenza di errore API o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.
7. Per salvare le modifiche, scegliere Salva modifiche.

CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi Insights, a condizione che vengano rilevate attività insolite durante quel periodo.

Registrazione degli eventi di Insights con AWS CLI

Puoi configurare i percorsi o i datastore di eventi per registrare gli eventi Insights utilizzando la AWS CLI.

> **Note**
>
> Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il trail o event data store deve registrare gli eventi di `write` gestione. Per registrare gli eventi di Insights sul

tasso di errore dell'API, il trail o event data store deve registrare `read` o `write` gestire gli eventi.

Argomenti

- Registrazione degli eventi di Insights per un percorso utilizzando il AWS CLI
- Registrazione degli eventi di Insights per un archivio dati di eventi utilizzando il AWS CLI

Registrazione degli eventi di Insights per un percorso utilizzando il AWS CLI

Per restituire i selettori attuali di Insights per un trail, esegui il `get-insight-selectors` comando.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

Il seguente esempio di risposta mostra i selettori Insights per un percorso denominato. `insights-trail`

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/insights-trail",
    "InsightSelectors": [
        {
            "InsightType": "ApiCallRateInsight"
        },
        {
            "InsightType": "ApiErrorRateInsight"
        }
    ]
}
```

Se il percorso non ha Insights abilitato, il get-insight-selectors comando restituisce il seguente messaggio di errore: «Si è verificato un errore (InsightNotEnabledException) durante la chiamata dell' GetInsightSelectors operazione: Trail arn:aws:cloudtrail:us-east- 1:123456789012:trail/trailName does not have Insights abilitato. Modificare le impostazioni del percorso per abilitare Insights, quindi riprovare l'operazione.»

Per configurare il percorso per la registrazione di eventi Insights, esegui il comando `put-insight-selectors`. Nell'esempio seguente viene illustrato come configurare il percorso per includere eventi Insights. I valori del selettore Insights possono essere`ApiCallRateInsight`, `ApiErrorRateInsight` o entrambi.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Il risultato seguente mostra il selettore di eventi Insights configurato per il trail.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
 }
```

Registrazione degli eventi di Insights per un archivio dati di eventi utilizzando il AWS CLI

Per registrare gli eventi di Insights in un datastore di eventi, è necessario un datastore di eventi di origine che registri gli eventi di gestione e un datastore di eventi di destinazione che registri gli eventi Insights.

Per vedere se gli eventi Insights sono abilitati su un datastore di eventi, esegui il comando get-insight-selectors.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Per vedere se un datastore di eventi è configurato per ricevere gli eventi Insights o gli eventi di gestione, esegui il comando get-event-data-store.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

Se un Event Data Store è configurato per ricevere eventi Insights, `eventCategory` verrà impostato `Insight` su.

Questa procedura mostra come creare i datastore di eventi di destinazione e di origine e come abilitare gli eventi Insights.

1. Esegui il comando aws cloudtrail create-event-data-store per creare un datastore di eventi di destinazione che raccolga gli eventi di Insights. Il valore di `eventCategory` deve essere `Insight`. Sostituiscilo *`retention-period-days`* con il numero di giorni in cui desideri conservare gli eventi nel tuo archivio dati degli eventi.

   Se hai effettuato l'accesso con l'account di gestione di un'organizzazione AWS Organizations , includi il parametro `--organization-enabled` se desideri consentire all'amministratore delegato l'accesso al datastore di eventi.

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

   Di seguito è riportata una risposta di esempio.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
```

```
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

Come valore per il parametro `--insights-destination` nel passaggio 3 utilizzerai l'ARN (o il suffisso ID dell'ARN) dalla risposta.

2. Esegui il comando aws cloudtrail create-event-data-store per creare un datastore di eventi di origine che registri gli eventi di gestione. Per impostazione predefinita, i datastore di eventi registrano tutti gli eventi di gestione. Non è necessario specificare i selettori di eventi avanzati se si desidera registrare tutti gli eventi di gestione. Sostituiscilo *`retention-period-days`* con il numero di giorni in cui desideri conservare gli eventi nel tuo archivio dati degli eventi. Se stai creando un datastore di eventi dell'organizzazione, includi il parametro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Come valore per il parametro `--event-data-store` nel passaggio 3 utilizzerai l'ARN (o il suffisso ID dell'ARN) dalla risposta.

3. Esegui il comando put-insight-selectors per abilitare gli eventi Insights. I valori del selettore Insights possono essere`ApiCallRateInsight`, `ApiErrorRateInsight` o entrambi. Per il parametro `--event-data-store`, specifica l'ARN (o il suffisso ID dell'ARN) del datastore di eventi di origine che registra gli eventi di gestione e abiliterà Insights. Per il parametro `--insights-destination`, specifica l'ARN (o il suffisso ID dell'ARN) del datastore di eventi di destinazione che registrerà gli eventi di Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Il risultato seguente mostra il selettore di eventi Insights configurato per il datastore di eventi.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
```

```
        },
        {
           "InsightType": "ApiCallRateInsight"
        }
     ]
}
```

Dopo aver abilitato CloudTrail Insights per la prima volta su un Event Data Store, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi di Insights, a condizione che durante quel periodo venga rilevata un'attività insolita.

Visualizzazione di eventi Insights per i percorsi

Questa sezione descrive come cercare negli ultimi 90 giorni di eventi Insights un percorso con CloudTrail Insights abilitato. Per informazioni su come visualizzare CloudTrail Insights per un data store di eventi, consultaVisualizzazione del dashboard di Insights per un data store di eventi.

Puoi visualizzare, filtrare e scaricare gli ultimi 90 giorni di eventi di Insights come percorso dalla pagina Insights sulla console.

Puoi cercare gli ultimi 90 giorni di eventi Insights in modo programmatico eseguendo il AWS CLI lookup-eventscomando o LookupEventsfunzionamento dell'API.

Per le descrizioni dei campi di registrazione degli eventi di Insights per i percorsi, vedereCloudTrail registra contenuti per gli eventi Insights per i percorsi.

> **Note**
>
> La pagina e il AWS CLI `lookup-events` comando Insights elencano gli eventi di Insights solo se hai abilitato Insights su un percorso che registra gli eventi di gestione. Per informazioni sull'attivazione di Insights su un percorso, consulta Abilitare CloudTrail Insights su un percorso esistente con la console eRegistrazione degli eventi di Insights per un percorso utilizzando il AWS CLI.
> Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il percorso deve registrare gli eventi di `write` gestione. Per registrare gli eventi di Insights in base al tasso di errore dell'API, il percorso deve registrare gli eventi `read` o gli eventi di `write` gestione.

Argomenti

- Visualizzazione degli eventi Insights per i percorsi con la console
- Visualizzazione degli eventi Insights per i sentieri con AWS CLI

Visualizzazione degli eventi Insights per i percorsi con la console

Questa sezione descrive come visualizzare, cercare e scaricare gli ultimi 90 giorni di eventi Insights per un percorso dalla pagina Insights sulla CloudTrail console. Per informazioni su come visualizzare CloudTrail Insights per un archivio dati di eventi, consultaVisualizzazione del dashboard di Insights per un data store di eventi.

Dopo aver registrato gli eventi di Insights per un percorso, gli eventi vengono visualizzati nella pagina Insights per 90 giorni. Non è possibile eliminare manualmente gli eventi dalla pagina Insights. Poiché gli eventi Insights abilitati per un trail sono archiviati nel bucket Amazon S3 configurato per quel trail, la rimozione degli eventi Insights dal bucket eliminerà tali eventi.

Puoi monitorare i log dei trail e ricevere notifiche quando si verificano eventi specifici di Insights abilitando i log. CloudWatch Per ulteriori informazioni, consulta Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs.

> **Note**
>
> CloudTrail Gli eventi Insights devono essere abilitati sul percorso per visualizzare gli eventi Insights nella console. Attendi fino a 36 ore CloudTrail per la distribuzione dei primi eventi Insights, a condizione che venga rilevata un'attività insolita durante quel periodo.
> Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il trail deve registrare gli eventi di `write` gestione. Per registrare gli eventi di Insights in base al tasso di errore dell'API, il percorso deve registrare gli eventi `read` o gli eventi di `write` gestione.

Per visualizzare gli eventi Insights

1. Accedi a AWS Management Console e apri la CloudTrail console a https://console.aws.amazon.com/cloudtrail/casa/.
2. Nel riquadro di navigazione, scegli Insights per visualizzare tutti gli eventi Insights registrati nel tuo account negli ultimi 90 giorni. Puoi anche visualizzare i cinque eventi Insights più recenti dalla pagina Dashboards.

3. Nella pagina Insights, puoi filtrare gli eventi di Insights in base all'origine dell'evento, al nome dell'evento o all'ID dell'evento. Per ulteriori informazioni sul filtro degli eventi Insights, consulta Filtro degli eventi Insights.
4. È possibile limitare ulteriormente l'elenco a un intervallo relativo o un intervallo assoluto.

Indice

- Filtro degli eventi Insights
- Visualizzazione dei dettagli degli eventi Insights
- Zoom, panoramica e download del grafico
- Modifica delle impostazioni dell'intervallo temporale del grafico
- Download di eventi Insights

Filtro degli eventi Insights

Per impostazione predefinita, gli eventi nella pagina Insights vengono visualizzati in ordine cronologico inverso in base all'ora di inizio dell'evento.

È possibile filtrare l'elenco scegliendo uno dei tre attributi seguenti:

Nome evento

Il nome dell'evento, in genere l' AWS API su cui sono stati registrati livelli di attività insoliti.

Origine eventi

Il AWS servizio a cui è stata effettuata la richiesta, ad esempio `iam.amazonaws.com` `os3.amazonaws.com`. Se scegli di filtrare in base all'origine degli eventi, puoi scorrere un elenco di fonti di eventi.

ID evento

L'ID dell'evento Insights. IDs Gli eventi non vengono visualizzati nella tabella delle pagine di Insights, ma sono un attributo in base al quale è possibile filtrare gli eventi di Insights. L'evento IDs degli eventi di gestione che vengono analizzati per generare eventi Insights è diverso dall'evento IDs degli eventi Insights.

L'elenco seguente descrive gli attributi di un evento, che non sono filtrabili:

Tipo di informazioni

Il tipo di evento CloudTrail Insights, che corrisponde alla frequenza delle chiamate API o al tasso di errore dell'API. Il tipo di approfondimento sulla frequenza delle chiamate API analizza le chiamate API di gestione in sola scrittura aggregate al minuto rispetto a un volume di chiamate API di base. Il tipo di approfondimento sul tasso di errore delle API analizza le chiamate API di gestione che generano codici di errore. L'errore viene visualizzato se la chiamata API non ha esito positivo.

Ora di inizio dell'evento

L'ora di inizio dell'evento Insights, misurata come il primo minuto in cui è stata registrata un'attività insolita. Questo attributo è mostrato nella tabella Insights, ma non puoi filtrare l'ora di inizio dell'evento nella console.

Media di base

La baseline rappresenta il modello normale di attività della frequenza delle chiamate o del tasso di errore delle API, calcolato giornalmente. La media di base è la media di queste linee di base giornaliere nei sette giorni precedenti l'inizio di un evento Insights. Sebbene questo periodo sia generalmente di sette giorni, CloudTrail arrotonda il periodo di calcolo a un numero intero di giorni, in modo che la durata di base esatta possa variare leggermente.

Media di informazioni

Il numero medio di chiamate a un'API o il numero medio di un errore specifico restituito nelle chiamate a un'API, che ha attivato l'evento Insights. La media di CloudTrail Insights per l'evento iniziale è la frequenza di occorrenze che hanno attivato l'evento Insights. In genere si tratta del primo minuto di attività insolita. La media di informazione per l'evento finale è la frequenza di chiamate API al minuto per la durata dell'attività insolita, tra l'evento Insights di inizio e di fine.

Cambio del tasso

La differenza tra il valore di Media di base e Media dell'informazione misurato come percentuale. Ad esempio, se la media di base di un errore `AccessDenied` che si verifica è 1,0 e la media di informazione è 3,0, la variazione del tasso è del 300%. Una variazione del tasso per una media di informazione che supera la media di base mostra una freccia superiore accanto al valore. Se l'evento Insights è stato registrato perché l'attività è inferiore alla media di base, Cambio di tasso mostra una freccia verso il basso accanto alla percentuale.

Se non sono presenti eventi registrati per l'attributo o l'intervallo di tempo scelto, l'elenco dei risultati è vuoto. È possibile applicare solo un filtro attributo oltre all'intervallo di tempo. Se si scegli un filtro attributo diverso, l'intervallo di tempo specificato viene conservato.

La procedura riportata di seguito illustra come filtrare i dati in base a un attributo.

Per filtrare in base un attributo

1. Per filtrare i risultati in base a un attributo, scegliete un attributo di ricerca dal menu a discesa, quindi digitate o scegliete un valore nella casella Inserisci un valore di ricerca.
2. Per rimuovere un filtro attributo, scegliere X a destra della casella del filtro attributo.

La procedura riportata di seguito illustra come filtrare in base alla data e all'ora di inizio e fine.

Per filtrare in base a una data e ora di inizio e fine

1. Da Filtra per data e ora, scegli una delle seguenti opzioni:
   - Intervallo assoluto: consente di scegliere un orario specifico. Passa alla fase successiva.
   - Intervallo relativo: selezionato per impostazione predefinita. Consente di scegliere un periodo di tempo relativo all'ora di inizio di un evento Insights. Proseguire con il passaggio 3.
2. Per impostare un intervallo assoluto, procedi come segue.
   a. Scegli il giorno in cui desideri che inizi l'intervallo di tempo. Inserisci un'ora di inizio nel giorno selezionato. Per inserire manualmente una data, digita la data nel formato `yyyy/mm/dd`. L'ora di inizio e di fine utilizzano un orologio di 24 ore e i valori devono essere nel formato `hh:mm:ss`. Ad esempio, per indicare un'ora di inizio alle 18:30, inserisci **`18:30:00`**.
   b. Scegli una data di fine per l'intervallo nel calendario oppure specifica una data e un'ora di fine al di sotto del calendario. Scegli Applica.
3. Per impostare un intervallo relativo, procedi come segue.
   a. Scegli un periodo di tempo preimpostato relativo all'ora di inizio di eventi Insights. Gli intervalli di tempo preimpostati includono 30 minuti, 1 ora, 12 ore o 1 giorno. Per specificare un intervallo di tempo personalizzato, scegli Custom (Personalizzato).
   b. Dopo aver impostato l'ora relativa che desideri, scegli Apply (Applica).
4. Per rimuovere un filtro per intervallo di tempo, scegli l'icona del calendario a destra della casella Filtra per data e ora, quindi scegli Cancella e ignora.

Visualizzazione dei dettagli degli eventi Insights

1. Scegliere un evento Insights nell'elenco dei risultati per visualizzare i relativi dettagli. La pagina dei dettagli di un evento Insights mostra un grafico della sequenza temporale dell'attività insolita.

2. Passa il puntatore del mouse sulle bande evidenziate per visualizzare l'ora di inizio e la durata di ogni evento Insights nel grafico.

   La seguente informazione è mostrata nell'area del grafico Informazioni aggiuntive:

   - Insight type (Tipo di informazioni). Può trattarsi di una frequenza di chiamata API o di un tasso di errore API.
   - Trigger. Questo è un collegamento alla scheda Cloudtrail events (Eventi Cloudtrail), che elenca gli eventi di gestione analizzati per determinare che si è verificata un'attività insolita.
   - Chiamate API al minuto o errori al minuto
     - Baseline average (Media di base) - La frequenza tipica di occorrenze al minuto su questa API, in cui l'evento Insight è stato registrato, misurata nei sette giorni precedenti circa, in una regione specifica dell'account.
     - Media Insights - La frequenza di occorrenze al minuto su questa API che hanno attivato l'evento Insights. La media CloudTrail Insights per l'evento di avvio è la frequenza di chiamate o errori al minuto sull'API che ha attivato l'evento Insights. In genere si tratta del primo minuto di attività insolita. La media Insights per l'evento di fine è la frequenza di chiamate API o errori al minuto per tutta la durata dell'attività insolita, tra l'evento Insights di inizio e l'evento Insights di fine.
   - Event source (Origine eventi). L'endpoint del AWS servizio su cui è stato registrato il numero insolito di chiamate o errori dell'API. Nell'immagine precedente, l'origine è`ec2.amazonaws.com`, che è l'endpoint del servizio per Amazon. EC2
   - ID evento di inizio - L'ID dell'evento Insights registrato all'inizio di attività insolita.
   - ID evento di fine - L'ID dell'evento Insights registrato al termine di attività insolita.
   - ID evento condiviso: negli eventi Insights, l'ID evento condiviso è un GUID generato da CloudTrail Insights per identificare in modo univoco una coppia di eventi Insights di inizio e fine. ID evento condiviso è comune tra gli eventi Insights di inizio e di fine e consente di creare una correlazione tra entrambi gli eventi per identificare in modo univoco l'attività insolita.

3. Seleziona la scheda Attributions (Attribuzioni) per visualizzare informazioni sulle identità utente, sugli agenti dell'utente, sugli eventi Insight del tasso di chiamate API e sui codici di errore correlati all'attività insolita e di riferimento. Sono visualizzati un massimo di cinque identità utente, cinque agenti dell'utente e cinque codici di errore nelle tabelle nella scheda Attributions (Attribuzioni), ordinati in base alla media del conteggio delle attività, in ordine decrescente dalla più alta alla più bassa.
4. Nella scheda CloudTrail eventi, visualizza gli eventi correlati CloudTrail analizzati per determinare che si è verificata un'attività insolita. Per impostazione predefinita, un filtro è già applicato per il nome dell'evento Insights, che è anche il nome dell'API correlata. La scheda CloudTrail eventi mostra gli eventi di CloudTrail gestione relativi all'API dell'oggetto che si sono verificati tra l'ora di inizio (meno un minuto) e l'ora di fine (più un minuto) dell'evento Insights.

   Quando si selezionano altri eventi di Insights nel grafico, gli eventi mostrati nella tabella degli CloudTrail eventi cambiano. Questi eventi ti permettono di eseguire analisi più approfondite per determinare la probabile causa di un evento Insights e i motivi di un'attività API insolita.

   Per mostrare tutti CloudTrail gli eventi che sono stati registrati durante la durata dell'evento Insights, e non solo quelli per l'API correlata, disattiva il filtro.
5. Seleziona la scheda Insights event record (Record di eventi Insights) per visualizzare gli eventi di inizio e di fine Insights in formato JSON.
6. Selezionando l'Event source (Origine eventi) collegata, puoi tornare alla pagina Insights, filtrata in base all'origine eventi.

Zoom, panoramica e download del grafico

È possibile eseguire lo zoom, la panoramica e il ripristino degli assi del grafico nella pagina dei dettagli dell'evento Insights utilizzando una barra degli strumenti nell'angolo in alto a destra.

Da sinistra a destra, i pulsanti di comando sulla barra degli strumenti del grafico effettuano le seguenti operazioni:

- Download plot as a PNG (Scarica grafico come PNG) – Carica l'immagine del grafico mostrata nella pagina dei dettagli e salvala in formato PNG.
- Zoom – Trascina per selezionare un'area del grafico da ingrandire e visualizzare nei minimi dettagli.
- Pan (Panoramica) – Sposta il grafico per visualizzare le date o le ore adiacenti.

- Reset axes (Ripristina assi) – Modifica gli assi del grafico ai valori originari, eliminando le impostazioni dello zoom e della panoramica.

Modifica delle impostazioni dell'intervallo temporale del grafico

Puoi modificare l'intervallo di tempo, ovvero la durata selezionata degli eventi visualizzati sull'asse x, mostrato nel grafico scegliendo un'impostazione nell'angolo superiore destro del grafico.

Download di eventi Insights

È possibile eseguire il download della cronologia degli eventi registrati come file in formato CSV o JSON. Utilizzare i filtri e gli intervalli di tempo per ridurre le dimensioni del file scaricato.

> **Note**
>
> CloudTrail i file di cronologia degli eventi sono file di dati che contengono informazioni (come i nomi delle risorse) che possono essere configurate dai singoli utenti. Alcuni dati potrebbero essere interpretati come comandi nei programmi utilizzati per leggere e analizzare questo tipo di informazioni (rischio di attacco di tipo CSV Injection o Formula Injection). Ad esempio, quando CloudTrail gli eventi vengono esportati in formato CSV e importati in un programma per fogli di calcolo, tale programma potrebbe avvisare l'utente in merito a problemi di sicurezza. Come best practice di sicurezza, è consigliabile disabilitare i collegamenti o le macro dai file scaricati della cronologia degli eventi.

1. Specificare il filtro e l'intervallo di tempo per gli eventi che si desidera scaricare. Ad esempio, è possibile specificare il nome dell'evento e specificare un intervallo di tempo per le ultime 12 ore di attività. `StartInstances`
2. Seleziona Download events (Download di eventi), quindi Download as CSV (Scarica in formato CSV) o Download as JSON (Scarica in formato JSON). Viene richiesto di scegliere una posizione in cui salvare il file.

> **Note**
>
> Il download potrebbe richiedere alcuni minuti per essere completato. Per ottenere più rapidamente i risultati, prima di avviare il processo di download, utilizzare un filtro più specifico o un intervallo di tempo più breve per limitare i risultati.

3. Al termine del download, aprire il file per visualizzare gli eventi specificati.
4. Per annullare il download, scegli Annulla. Se annulli un download prima che sia terminato, un file CSV o JSON nel computer locale potrebbe contenere solo una parte degli eventi.

Visualizzazione degli eventi Insights per i sentieri con AWS CLI

Questa sezione descrive come utilizzare il AWS CLI `lookup-events` comando per cercare gli ultimi 90 giorni di eventi Insights per un percorso con gli eventi Insights abilitati. Per informazioni su come abilitare CloudTrail Insights su un percorso, consultaRegistrazione degli eventi di Insights per un percorso utilizzando il AWS CLI.

> **Note**
>
> Non è possibile utilizzare il `lookup-events` comando per cercare gli eventi di Insights per un data store di eventi, tuttavia CloudTrail Lake offre una serie di query di esempio per gli archivi di dati di eventi Insights. Per ulteriori informazioni, consulta Visualizzazione di query di esempio per gli eventi Insights.

Il comando `lookup-events` ha le seguenti opzioni:

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`

- `--cli-input-json`

Per informazioni generali sull'utilizzo di AWS Command Line Interface, consulta la Guida per l'AWS Command Line Interface utente.

Indice

- Prerequisiti
- Visualizzazione delle informazioni di aiuto della riga di comando
- Ricerca degli eventi Insights
- Specificare il numero di eventi Insights da restituire
- Ricerca degli eventi Insights per intervallo di tempo
- Ricerca degli eventi Insights per attributo
  - Esempi di ricerca in base a un attributo
- Specifica della pagina di risultati successiva
- Recupero dell'input JSON da un file
- Campi di output della ricerca

Prerequisiti

- Per eseguire AWS CLI i comandi, è necessario installare AWS CLI. Per ulteriori informazioni, consulta la Guida introduttiva a AWS CLI.
- Assicurati che la tua AWS CLI versione sia successiva alla 1.6.6. Per verificare la versione della CLI, esegui aws --version nella riga di comando.
- Per impostare l'account, la regione e il formato di output predefinito per una AWS CLI sessione, usa il aws configure comando. Per ulteriori informazioni, consulta Configurazione di AWS Command Line Interface.
- Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il trail deve registrare gli eventi di `write` gestione. Per registrare gli eventi di Insights in base al tasso di errore dell'API, il percorso deve registrare gli eventi `read` o gli eventi di `write` gestione.

> **Note**
>
> I CloudTrail AWS CLI comandi fanno distinzione tra maiuscole e minuscole.

Visualizzazione delle informazioni di aiuto della riga di comando

Per visualizzare le informazioni di aiuto della riga di comando per `lookup-events`, digita il comando seguente.

```
aws cloudtrail lookup-events help
```

Ricerca degli eventi Insights

Per visualizzare i dieci eventi Insights più recenti, digita il comando seguente.

```
aws cloudtrail lookup-events --event-category insight
```

Un evento restituito è simile all'esempio che segue,


```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:52:00Z",
            "awsRegion": "us-east-1",
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
```

```
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:53:00Z",
            "awsRegion": "us-east-1",
            "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "End",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
```

```
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 6
                        },
                        "insightDuration": 1,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        }
    ]
}
```

Per una spiegazione dei campi correlati alla ricerca nell'output, vedere la sezione Campi di output della ricerca. Per una spiegazione di campi nell'evento Insights, consulta CloudTrail registra contenuti per gli eventi Insights per i percorsi.

Specificare il numero di eventi Insights da restituire

Per specificare il numero di eventi da restituire, digita il comando seguente.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

Il valore predefinito per`<integer>`, se non è specificato, è 10. I valori possibili sono da 1 a 50. L'esempio seguente restituisce un risultato.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

Ricerca degli eventi Insights per intervallo di tempo

Gli eventi Insights degli ultimi 90 giorni sono disponibili per la ricerca. Per specificare un intervallo di tempo, digita il comando seguente.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time <timestamp>` specifica, in UTC, che vengono restituiti solo gli eventi Insights che si sono verificati in corrispondenza o dopo l'intervallo di tempo specificato. Se l'ora di inizio specificata è successiva all'ora di fine specificata, viene restituito un errore.

`--end-time <timestamp>` specifica, in UTC, che vengono restituiti solo gli eventi Insights che si sono verificati in corrispondenza o prima dell'intervallo di tempo specificato. Se l'ora di fine specificata è anteriore all'ora di inizio specificata, viene restituito un errore.

L'ora di inizio di default è la prima data in cui i dati sono disponibili negli ultimi 90 giorni. L'ora di fine di default è invece l'ora dell'evento che si è verificato più in vicinanza dell'ora corrente.

Tutti i timestamp sono mostrati in UTC.

Ricerca degli eventi Insights per attributo

Per filtrare in base a un attributo, digita il comando seguente.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Puoi specificare solo una coppia chiave/valore attributo per ogni comando lookup-events. Di seguito sono riportati i valori degli eventi Insights validi per `AttributeKey`. I nomi dei valori fanno distinzione tra lettere maiuscole e minuscole.

- `EventId`
- `EventName`
- `EventSource`

La lunghezza massima per `AttributeValue` è di 2000 caratteri. I seguenti caratteri ('_', ' ', ',', '\ \n') contano come due caratteri nel limite di 2000 caratteri.

Esempi di ricerca in base a un attributo

Il comando di esempio seguente restituisce gli eventi Insights in cui il valore di `EventName` è `PutRule`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Il comando di esempio seguente restituisce gli eventi Insights in cui il valore di `EventId` è `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Il comando di esempio seguente restituisce gli eventi Insights in cui il valore di `EventSource` è `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

Specifica della pagina di risultati successiva

Per visualizzare la pagina di risultati successiva mediante un comando `lookup-events`, digita il comando seguente,

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

In questo comando, il valore di *<token>* viene preso dal primo campo dell'output del comando precedente.

Quando utilizzi `--next-token` in un comando, devi utilizzare gli stessi parametri usati nel comando precedente. Ad esempio, supponiamo che tu abbia eseguito il seguente comando.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Per visualizzare la pagina di risultati successiva, il comando successivo avrà l'aspetto seguente.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Recupero dell'input JSON da un file

AWS CLI Per alcuni AWS servizi ha due parametri, `--generate-cli-skeleton` uno dei quali è possibile utilizzare per generare un modello JSON, che è possibile modificare e utilizzare come input per il `--cli-input-json` parametro. `--cli-input-json` Questa sezione descrive come utilizzare questi parametri con `aws cloudtrail lookup-events`. Per ulteriori informazioni, consultate AWS CLI scheletri e file di input.

Per cercare eventi Insights recuperando l'input JSON da un file

1. Crea un modello di input da usare con `lookup-events` reindirizzando l'output di `--generate-cli-skeleton` in un file, come nell'esempio seguente.

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   Il file modello generato (in questo caso, LookupEvents .txt) ha l'aspetto seguente.

   ```
   {
       "LookupAttributes": [
   ```

```
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Utilizza un editor di testo per modificare l'input JSON in base alle esigenze. L'input JSON deve contenere solo i valori specificati.

> **Important**
>
> Tutti i valori vuoti o null devono essere rimossi dal modello prima di utilizzarlo.

L'esempio seguente specifica un intervallo di tempo e il numero massimo di risultati da restituire.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Per utilizzare il file modificato come input, utilizzate la sintassi `--cli-input-json file://<filename>`, come nell'esempio seguente.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> Puoi utilizzare altri argomenti sulla stessa riga di comando come `--cli-input-json`.

Campi di output della ricerca

Eventi

Un elenco di eventi di ricerca in base all'attributo di ricerca e all'intervallo di tempo specificati. L'elenco di eventi è ordinato in base all'ora, con l'ultimo evento elencato per primo. Ogni voce contiene informazioni sulla richiesta di ricerca e include una rappresentazione in formato stringa dell' CloudTrail evento recuperato.

Le voci seguenti descrivono i campi in ogni evento di ricerca.

CloudTrailEvent

Stringa JSON contenente una rappresentazione oggetto dell'evento restituito. Per informazioni su ciascuno degli elementi restituiti, consulta l'argomento relativo al contenuto del corpo dei record.

EventId

Stringa contenente il GUID dell'evento restituito.

EventName

Stringa contenente il nome dell'evento restituito.

EventSource

Il AWS servizio a cui è stata effettuata la richiesta.

EventTime

Data e ora, in formato UNIX, dell'evento.

Risorse

Elenco delle risorse a cui fa riferimento l'evento restituito. Ogni voce specifica un tipo e un nome di risorsa.

ResourceName

Stringa contenente il nome della risorsa a cui l'evento fa riferimento.

ResourceType

Stringa contenente il tipo di una risorsa a cui l'evento fa riferimento. Quando risulta impossibile determinare il tipo di risorsa, viene restituito un valore null.

Nome utente

Stringa contenente il nome utente dell'account per l'evento restituito.

NextToken

Stringa per visualizzare la pagina di risultati successiva generata da un precedente comando `lookup-events`. Per usare il token, i parametri devono essere uguali a quelli specificati nel comando originale. Se nell'output non è presente alcuna voce `NextToken`, significa che non sono presenti altri risultati da restituire.

Per ulteriori informazioni sugli eventi CloudTrail Insights, Lavorare con CloudTrail Insights consulta questa guida.

Visualizzazione degli eventi Insights per i datastore di eventi

Questa sezione descrive come visualizzare gli eventi di Insights per un data store di eventi Insights visualizzando il dashboard degli eventi di Insights ed eseguendo query di esempio. Per informazioni su come abilitare CloudTrail Insights su un data store di eventi, consultaAbilitazione di CloudTrail Insights su un data store di eventi esistente con la console.

CloudTrail le query comportano addebiti in base alla quantità di dati scansionati. Per semplificare il controllo dei costi, consigliamo di vincolare le query aggiungendovi marche temporali `eventTime` di inizio e di fine. Per ulteriori informazioni sui prezzi di CloudTrail, consulta Prezzi di AWS CloudTrail.

Per le descrizioni dei campi di registrazione degli eventi di Insights per gli archivi dati degli eventi, vedere. CloudTrail registra i contenuti per gli eventi Insights per i datastore di eventi Lake.

Argomenti

- Visualizzazione del dashboard di Insights per un data store di eventi
- Visualizzazione di query di esempio per gli eventi Insights

Visualizzazione del dashboard di Insights per un data store di eventi

La dashboard degli eventi di Insights mostra la proporzione complessiva di eventi Insights per tipo di Insights, la proporzione di eventi Insights per tipo di Insights per gli utenti e i servizi principali e il numero di eventi Insights al giorno. Il pannello di controllo include anche un widget che riporta fino a 30 giorni di eventi Insights.

> **Note**
>
> - Dopo aver abilitato CloudTrail Insights per la prima volta nell'archivio dati degli eventi di origine, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi di Insights, a condizione che venga rilevata un'attività insolita durante quel periodo. Per ulteriori informazioni, consulta Erogazione di eventi Insights.
> - Il dashboard degli eventi di Insights mostra solo le informazioni sugli eventi di Insights raccolti dal data store degli eventi selezionato, che è determinato dalla configurazione del data store degli eventi di origine. Ad esempio, se configuri il datastore di eventi di origine per abilitare gli eventi Insights su `ApiCallRateInsight` ma non su `ApiErrorRateInsight`, non vedrai le informazioni sugli eventi Insights su `ApiErrorRateInsight`.

Per visualizzare il dashboard degli eventi di Insights

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. Dalle dashboard AWS gestite, scegli la dashboard degli eventi di Insights.
5. Scegli il tuo data store di eventi Insights.
6. Puoi decidere di filtrare i dati del pannello di controllo in base a un Intervallo assoluto o un Intervallo relativo. Scegli Intervallo assoluto per selezionare un intervallo di data e ora specifico. Scegli Intervallo relativo per selezionare un intervallo di tempo predefinito o un intervallo personalizzato. Per impostazione predefinita, il pannello di controllo mostra i dati di eventi delle ultime 24 ore.

   > **Note**
   >
   > CloudTrail Le query sul lago comportano costi in base alla quantità di dati scansionati. Per controllare i costi, puoi filtrare in base a un intervallo di tempo più ristretto. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

7. Scegli l'icona di aggiornamento per popolare la grafica dei widget della dashboard. Ogni widget indica lo stato dell'aggiornamento.

Per ulteriori informazioni sui pannelli di controllo di Lake, consulta CloudTrail Cruscotti Lake.

Visualizzazione di query di esempio per gli eventi Insights

La CloudTrail console fornisce una serie di query di esempio per gli eventi di Insights che possono aiutarti a iniziare a scrivere le tue query.

Per visualizzare query di esempio per gli eventi Insights

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, in Lake, scegli Query.
3. Nella pagina Query, scegli la scheda Sample queries (Query di esempio).
4. Cerca le query relative agli eventi Insights. Scegliete il nome della query per aprirla nella scheda Editor.

5. Nella scheda Editor, scegli l'archivio dati degli eventi Insights. Quando scegli il data store degli eventi dall'elenco, compila CloudTrail automaticamente l'ID del data store degli eventi nella `FROM` riga dell'editor di query.
6. Per eseguire la query, scegli Esegui. Al termine della query, è possibile visualizzare l'output del comando e i risultati della query.

   La scheda Output del comando mostra i metadati relativi alla query, ad esempio se la query ha avuto esito positivo, il numero di record corrispondenti e la durata di esecuzione della query.

   La scheda Risultati della query mostra i dati degli eventi nel datastore di eventi selezionato che corrispondono alla query.

Per ulteriori informazioni sulla modifica di una query, consulta Crea o modifica un'interrogazione con la console CloudTrail . Per ulteriori informazioni sull'esecuzione di una query e sul salvataggio dei relativi risultati, consulta Esegui una query e salva i risultati della query con la console.

Lavorare con AWS CloudTrail Lake

AWS CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili in base ai criteri selezionati applicando i selettori di eventi avanzati. Puoi conservare i dati degli eventi in un datastore di eventi per un massimo di 3.653 giorni (circa 10 anni) se scegli l'opzione Prezzo per la conservazione estendibile di un anno o di 2.557 giorni (circa 7 anni) se scegli l'opzione Prezzo per la conservazione di sette anni. I selettori che applichi a un event data store controllano quali eventi persistono e sono disponibili per essere interrogati. CloudTrail Lake è una soluzione di audit che può completare il vostro stack di conformità e aiutarvi nella risoluzione dei problemi quasi in tempo reale.

CloudTrail Archivi di dati sugli eventi Lake

Quando crei un archivio di dati degli eventi, scegli il tipo di eventi da includere in tale archivio. È possibile creare un archivio dati di eventi per includere CloudTrail eventi (eventi di gestione, eventi relativi ai dati, eventi di attività di rete), eventi CloudTrail Insights, elementi di AWS Config configurazione, AWS Audit Manager prove o eventi esterni a AWS. Ogni archivio dati di eventi può contenere solo una categoria di eventi specifica (ad esempio, elementi di AWS Config configurazione), poiché lo schema degli eventi è unico per la categoria di eventi. È possibile archiviare gli eventi di un'organizzazione AWS Organizations in un archivio dati di eventi organizzativi, inclusi gli eventi provenienti da più regioni e account. Puoi anche eseguire query SQL su più datastore di eventi utilizzando le parole chiave SQL JOIN supportate. Per informazioni sull'esecuzione di query su più datastore di eventi, consulta Supporto avanzato per query multi-tabella.

È possibile copiare gli eventi del trail in un data store di eventi nuovo o esistente per creare un' point-in-timeistantanea degli eventi registrati nel percorso. Per ulteriori informazioni, consulta Copia di eventi traccia in un archivio dati degli eventi.

Puoi eseguire la federazione di un datastore di eventi per visualizzare i metadati associati al datastore nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi utilizzando Amazon Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

Puoi allegare una policy basata sulle risorse al tuo archivio dati di eventi per fornire l'accesso tra più account a principali selezionati. Puoi aggiungere una policy basata sulle risorse quando crei o aggiorni un event data store sulla console o eseguendo il CloudTrail comando. AWS CLI `put-resource-policy` Per ulteriori informazioni, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

Per impostazione predefinita, tutti gli eventi in un archivio dati di eventi sono crittografati da. CloudTrail Quando configuri un Event Data Store, puoi scegliere di utilizzare la tua AWS Key Management Service chiave. L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

Puoi controllare l'accesso alle operazioni sui datastore di eventi utilizzando l'autorizzazione basata sui tag. Per ulteriori informazioni e degli esempi, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag in questa guida.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

CloudTrail Lake supporta le CloudWatch metriche di Amazon, che forniscono informazioni sui dati acquisiti e sui byte di archiviazione. Per ulteriori informazioni sulle metriche supportate CloudWatch , consulta. CloudWatch Metriche supportate

> **Note**
>
> CloudTrail in genere fornisce eventi entro una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito.

CloudTrail Domande sul lago

CloudTrail Le query su Lake offrono una visione più approfondita e personalizzabile degli eventi rispetto alle semplici ricerche di chiavi e valori nella cronologia degli eventi o in corso. `LookupEvents` Una ricerca nella cronologia degli eventi è limitata a una sola Account AWS, restituisce solo gli eventi di un singolo Regione AWS evento e non può interrogare più attributi. Al contrario, gli utenti di CloudTrail Lake possono eseguire query SQL complesse su più campi di

eventi. CloudTrail Lake supporta tutte le `SELECT` istruzioni e le funzioni Trino valide. Per ulteriori informazioni sulle funzioni e gli operatori SQL supportati, consulta Funzioni e operatori sul sito Web della documentazione di Trino.

È possibile creare una query nella scheda CloudTrail Lake Editor scrivendola da zero in SQL, aprendo una query salvata o di esempio e modificandola, oppure utilizzando il generatore di query per produrre una query da un prompt in lingua inglese. Per ulteriori informazioni, consultare Crea o modifica un'interrogazione con la console CloudTrail e Crea query su CloudTrail Lake da istruzioni in linguaggio naturale.

Puoi salvare le query di CloudTrail Lake per utilizzi futuri e visualizzare i risultati delle query per un massimo di sette giorni. Quando esegui query, è possibile salvare i risultati della query in un bucket Amazon S3.

La CloudTrail console fornisce una serie di query di esempio che possono aiutarti a iniziare a scrivere le tue query. Per ulteriori informazioni, consulta Visualizza query di esempio con la console CloudTrail .

CloudTrail Le richieste sul lago sono a pagamento. Quando si eseguono le query in Lake, si paga in base alla quantità di dati scansionati. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

CloudTrail Dashboard Lake

Puoi utilizzare le dashboard di CloudTrail Lake per visualizzare le tendenze degli eventi per gli archivi di dati sugli eventi presenti nel tuo account. CloudTrail Lake offre i seguenti tipi di dashboard:

- Dashboard gestiti: puoi visualizzare una dashboard gestita per visualizzare le tendenze degli eventi per un data store di eventi che raccoglie eventi di gestione, eventi relativi ai dati o eventi Insights. Queste dashboard sono automaticamente disponibili per te e sono gestite da Lake. CloudTrail CloudTrail offre 14 dashboard gestite tra cui scegliere. Puoi aggiornare manualmente i dashboard gestiti. Non è possibile modificare, aggiungere o rimuovere i widget per questi dashboard, tuttavia, è possibile salvare un dashboard gestito come dashboard personalizzato se si desidera modificare i widget o impostare una pianificazione di aggiornamento.
- Dashboard personalizzati: i dashboard personalizzati consentono di interrogare gli eventi in qualsiasi tipo di archivio dati di eventi. Puoi aggiungere fino a 10 widget a una dashboard personalizzata. Puoi aggiornare manualmente una dashboard personalizzata oppure impostare una pianificazione di aggiornamento.

- Dashboard Highlights: abilita la dashboard Highlights per visualizzare una at-a-glance panoramica dell' AWS attività raccolta dagli archivi di dati sugli eventi presenti nel tuo account. La dashboard Highlights è gestita CloudTrail e include widget pertinenti al tuo account. I widget mostrati nella dashboard Highlights sono unici per ogni account. Questi widget potrebbero far emergere attività o anomalie rilevate. Ad esempio, la dashboard Highlights potrebbe includere il widget Total cross-account access, che mostra se c'è un aumento delle attività anomale tra account. CloudTrail aggiorna la dashboard Highlights ogni 6 ore. La dashboard mostra i dati delle ultime 24 ore dall'ultimo aggiornamento.

Ogni dashboard è composta da uno o più widget e ogni widget rappresenta una query SQL.

Per ulteriori informazioni, consulta CloudTrail Cruscotti Lake.

CloudTrail Integrazioni Lake

Puoi utilizzare le integrazioni di CloudTrail Lake per registrare e archiviare i dati sulle attività degli utenti dall'esterno AWS; da qualsiasi fonte nei tuoi ambienti ibridi, come applicazioni interne o SaaS ospitate in locale o nel cloud, macchine virtuali o contenitori. Dopo aver creato gli archivi di dati degli eventi in CloudTrail Lake e creato un canale per registrare gli eventi di attività, chiami l'`PutAuditEvents`API per inserire l'attività dell'applicazione. CloudTrail Puoi quindi utilizzare CloudTrail Lake per cercare, interrogare e analizzare i dati registrati dalle tue applicazioni.

Le integrazioni possono anche registrare gli eventi negli archivi di dati degli eventi provenienti da oltre una CloudTrail dozzina di partner. In un'integrazione dei partner, crei degli archivi di dati degli eventi di destinazione, un canale e una policy delle risorse. Dopo aver creato l'integrazione, fornisci l'ARN del canale al partner. Esistono due tipi di integrazione: diretta e di soluzione. Con le integrazioni dirette, il partner chiama l'`PutAuditEvents`API per inviare eventi all'archivio dati degli eventi relativo al tuo account. AWS Con le integrazioni di soluzioni, l'applicazione viene eseguita nell' AWS account dell'utente e richiama l'`PutAuditEvents`API per inviare gli eventi all'archivio dati degli eventi relativo all'account AWS .

Per ulteriori informazioni sulle integrazioni, consulta Creare un'integrazione con una fonte di eventi esterna a. AWS

Risorse aggiuntive

Le seguenti risorse possono aiutarti a comprendere meglio cos'è CloudTrail Lake e come puoi usarlo.

- Modernizzate la gestione dei registri di controllo utilizzando CloudTrail Lake (YouTube video)
- Registra gli eventi di attività provenienti da AWS fonti diverse in AWS CloudTrail Lake (YouTube video)
- Analizza i registri delle attività con AWS CloudTrail Lake e Amazon Athena YouTube (video)
- Ottieni visibilità nei registri delle attività per la tua forza lavoro e le identità dei clienti (blog)AWS
- Utilizzo di AWS CloudTrail Lake per identificare le vecchie connessioni TLS agli endpoint di AWS servizio (blog)AWS
- In che modo Arctic Wolf utilizza AWS CloudTrail Lake per semplificare la sicurezza e le operazioni (blog)AWS
- CloudTrail Lago FAQs
- AWS CloudTrail Documentazione di riferimento delle API
- AWS CloudTrail Riferimento all'API dei dati
- AWS CloudTrail Guida all'onboarding dei partner

CloudTrail Regioni supportate dai laghi

Attualmente, CloudTrail Lake è supportato nelle seguenti aree Regioni AWS:

Nome della regione	Regione
US East (N. Virginia)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
Stati Uniti occidentali (California settentrionale)	us-west-1
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacifico (Hong Kong)	ap-east-1
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4

Nome della regione	Regione
Asia Pacific (Mumbai)	ap-south-1
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europa (Francoforte)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europa (Milano)	eu-south-1
Europe (Paris)	eu-west-3
Europa (Spagna)	eu-south-2
Europa (Stoccolma)	eu-north-1
Europa (Zurigo)	eu-central-2
Israele (Tel Aviv)	il-central-1
Medio Oriente (Bahrein)	me-south-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1
Sud America (São Paulo)	sa-east-1
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1

Nome della regione	Regione
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1

Per informazioni sugli endpoint CloudTrail del servizio, consulta AWS CloudTrail endpoints and quotas.

Per ulteriori informazioni sull'utilizzo CloudTrail in AWS GovCloud (US) Regions, consulta Service Endpoints nella Guida per l'utente.AWS GovCloud (US)

CloudTrail Concetti e terminologia dei laghi

Questa sezione descrive i concetti e i termini chiave per aiutarti a usare AWS CloudTrail Lake.

Concetti e termini

- Datastore di eventi
- Integrazioni
- Query
- Pannelli di controllo

Datastore di eventi

Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili in base ai criteri selezionati applicando i selettori di eventi avanzati.

È possibile creare un Event Data Store per registrare CloudTrail eventi (eventi di gestione, eventi relativi ai dati, eventi di attività di rete), eventi CloudTrail Insights, AWS Audit Manager prove, elementi di AWS Config configurazione o eventi esterni a AWS.

Selettori di eventi avanzati

I selettori di eventi avanzati determinano gli eventi da includere in un datastore di eventi. I selettori di eventi avanzati ti consentono di controllare i costi registrando solo gli eventi più importanti.

Per gli eventi di gestione, gli eventi relativi ai dati e gli eventi di attività di rete, puoi utilizzare selettori di eventi avanzati per filtrare gli eventi. Ad esempio, se stai creando un data store di

eventi per raccogliere eventi di gestione, puoi filtrare AWS Key Management Service (AWS KMS) o gli eventi dell'Amazon Relational Database Service (Amazon RDS) Data API. In genere, AWS KMS azioni come `Encrypt` e `GenerateDataKey` generano oltre il 99 percento degli eventi. `Decrypt`

Per gli elementi di AWS Config configurazione, le evidenze dell'Audit Manager o gli eventi esterni AWS, i selettori di eventi avanzati vengono utilizzati solo per includere eventi di quel tipo nell'archivio dati degli eventi.

Federazione

La federazione consente di visualizzare i metadati associati a un data store di eventi nel AWS Glue Data Catalog ed eseguire query SQL sui dati dell'evento utilizzando Amazon Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare.

Quando abiliti la federazione delle query di Lake, CloudTrail crea le risorse federate per tuo conto e le registra con. AWS Lake Formation Dopo aver abilitato la federazione di Data Lake, puoi eseguire query direttamente sui dati degli eventi in Athena senza dover eseguire passaggi aggiuntivi. Per ulteriori informazioni, consulta Federare un datastore di eventi.

Opzione di prezzo

Quando crei un datastore di eventi, scegli l'opzione di prezzo che desideri utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il datastore di eventi. Per informazioni sui prezzi, consulta Prezzo AWS CloudTrail e Gestione dei costi CloudTrail del lago.

Periodo di conservazione

Il periodo di conservazione di un Event Data Store determina per quanto tempo i dati degli eventi vengono conservati nell'Event Data Store. CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

Periodo di conservazione predefinito

Il periodo di conservazione predefinito di un datastore di eventi è il numero predefinito di giorni per cui i dati degli eventi vengono conservati nel datastore. Durante il periodo di conservazione predefinito di un datastore di eventi, l'archiviazione è inclusa nel prezzo di importazione senza

costi aggiuntivi. Dopo il periodo di conservazione predefinito, il prezzo per l'archiviazione è pay-as-you-go.

Periodo di conservazione massimo

Il periodo di conservazione massimo di un datastore di eventi rappresenta il numero massimo di giorni per cui è possibile conservare i dati in un datastore.

Termination protection (Protezione da cessazione)

Per impostazione predefinita, i datastore prevedono l'abilitazione della protezione della terminazione per evitare l'eliminazione accidentale. Per eliminare un datastore di eventi con la protezione della terminazione abilitata, scegli Modifica la protezione della terminazione dal menu Operazioni nella pagina dei dettagli del datastore. Quindi puoi procedere con l'eliminazione del datastore di eventi. Per ulteriori informazioni, consulta Modificare la protezione dalla terminazione con la console.

Integrazioni

Puoi utilizzare le integrazioni di CloudTrail Lake per registrare e archiviare i dati sulle attività degli utenti dalle seguenti fonti:

- Al di fuori di AWS
- Qualsiasi origine nei tuoi ambienti ibridi, ad esempio applicazioni interne o software as a service (SaaS) ospitate on-premise o nel cloud, macchine virtuali o container

Per ricevere eventi, un'integrazione richiede un canale per la distribuzione degli eventi e un datastore di eventi. Dopo aver configurato l'integrazione, richiama l'operatore dell'PutAuditEventsAPI per importare l'attività dell'applicazione. CloudTrail Quindi, puoi usare CloudTrail Lake per cercare, interrogare e analizzare i dati registrati dalle tue applicazioni. Per ulteriori informazioni, consulta Crea un'integrazione con una fonte di eventi esterna a AWS.

Tipo di integrazione

Esistono due tipi di integrazione: diretta e soluzione. Con le integrazioni dirette, il partner chiama l'operazione API `PutAuditEvents` per distribuire gli eventi al datastore di eventi per il tuo Account AWS. Con le integrazioni di soluzioni, l'applicazione viene eseguita all'interno dell'utente Account AWS e richiama l'operazione `PutAuditEvents` API per fornire gli eventi all'archivio dati degli eventi per conto dell'utente. Account AWS

Canali

Attiva gli eventi da fonti esterne al AWS lavoro utilizzando i canali per portare eventi in CloudTrail Lake da partner esterni che collaborano con CloudTrail o provenienti dalle tue fonti. Quando crei un canale, scegli uno o più archivi di dati degli eventi per archiviare gli eventi che provengono dall'origine del canale. È possibile modificare gli archivi di dati degli eventi di destinazione per un canale in base alle esigenze, a condizione che tali archivi siano impostati per registrare gli eventi `eventCategory="ActivityAuditLog"`. Quando crei un canale per gli eventi provenienti da un partner esterno, fornisci un nome della risorsa Amazon (ARN) di canale al partner o all'applicazione di origine.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. La policy basata su risorse collegata al canale consente all'origine di trasmettere eventi attraverso il canale. Se un canale non dispone di una policy delle risorse, solo il proprietario del canale può chiamare l'operazione API `PutAuditEvents` sul canale. Per ulteriori informazioni, consulta AWS CloudTrail esempi di policy basate sulle risorse.

Query

Le query in CloudTrail Lake sono create in SQL. È possibile creare una query nella scheda CloudTrail Lake Editor scrivendola da zero in SQL, aprendo una query salvata o di esempio e modificandola oppure utilizzando il generatore di query per produrre una query da un prompt in lingua inglese. Per ulteriori informazioni, consultare Crea o modifica un'interrogazione con la console CloudTrail e Crea query su CloudTrail Lake da istruzioni in linguaggio naturale.

CloudTrail Lake supporta tutte le Trino `SELECT` istruzioni e le funzioni valide. Per ulteriori informazioni sulle funzioni e gli operatori SQL supportati, consulta Funzioni e operatori sul sito Web della documentazione di Trino.

Pannelli di controllo

Utilizzando le dashboard di CloudTrail Lake, puoi visualizzare gli eventi in un data store di eventi e vedere le tendenze degli eventi, ad esempio i top Servizi AWS, gli utenti e gli errori. Per ulteriori informazioni, consulta CloudTrail Cruscotti Lake.

Tipi di dashboard

CloudTrail Lake offre i seguenti tipi di dashboard:

- Dashboard gestiti: puoi visualizzare una dashboard gestita per visualizzare le tendenze degli eventi per un data store di eventi che raccoglie eventi di gestione, eventi relativi ai dati o eventi Insights. Queste dashboard sono automaticamente disponibili per te e sono gestite da Lake. CloudTrail CloudTrail offre 14 dashboard gestite tra cui scegliere. Puoi aggiornare manualmente i dashboard gestiti. Non è possibile modificare, aggiungere o rimuovere i widget per questi dashboard, tuttavia, è possibile salvare un dashboard gestito come dashboard personalizzato se si desidera modificare i widget o impostare una pianificazione di aggiornamento.
- Dashboard personalizzati: i dashboard personalizzati consentono di interrogare gli eventi in qualsiasi tipo di archivio dati di eventi. Puoi aggiungere fino a 10 widget a una dashboard personalizzata. Puoi aggiornare manualmente una dashboard personalizzata oppure impostare una pianificazione di aggiornamento.
- Dashboard Highlights: abilita la dashboard Highlights per visualizzare una at-a-glance panoramica dell' AWS attività raccolta dagli archivi di dati sugli eventi presenti nel tuo account. La dashboard Highlights è gestita CloudTrail e include widget pertinenti al tuo account. I widget mostrati nella dashboard Highlights sono unici per ogni account. Questi widget potrebbero far emergere attività o anomalie rilevate. Ad esempio, la dashboard Highlights potrebbe includere il widget Total cross-account access, che mostra se c'è un aumento delle attività anomale tra account. CloudTrail aggiorna la dashboard Highlights ogni 6 ore. La dashboard mostra i dati delle ultime 24 ore dall'ultimo aggiornamento.

Widget

I widget sono i componenti che costituiscono una dashboard e forniscono una visualizzazione, ad esempio un grafico a linee o un grafico a barre. Ogni widget corrisponde a una query SQL. Quando aggiorni una dashboard, CloudTrail esegue una query per ogni widget sulla dashboard per compilare i dati relativi al widget.

CloudTrail Archivi di dati sugli eventi di Lake

Quando crei un data store di eventi in CloudTrail Lake, scegli il tipo di eventi da includere nel tuo archivio dati di eventi. Puoi creare un data store di eventi per includere CloudTrail eventi (eventi di gestione, eventi di dati o eventi di attività di rete), eventi CloudTrail Insights, elementi di AWS Config configurazione o eventi esterni a AWS. Ogni tipo di archivio dati di eventi può contenere solo categorie di eventi specifiche (ad esempio, elementi di AWS Config configurazione), poiché lo schema degli eventi è unico per la categoria di eventi. Puoi eseguire query SQL su più datastore di eventi utilizzando le parole chiave SQL JOIN supportate. Per informazioni sull'esecuzione di query su più datastore di eventi, consulta Supporto avanzato per query multi-tabella.

Nella tabella seguente vengono illustrate le categorie di eventi supportate per ciascun tipo di datastore di eventi. La colonna eventCategory mostra il valore da specificare nei selettori di eventi avanzati per raccogliere eventi di quel tipo.

Tipo di evento (console)	eventCategory (API)	Descrizione

CloudTrail eventi	`Management`
	`Data`
	`NetworkActivity`
		Questo tipo di archivio dati di eventi può raccogliere eventi di CloudTrail gestione, eventi di dati ed eventi di attività di rete. Per ulteriori informazioni, consulta Creare un archivio dati di CloudTrail eventi per gli eventi.

CloudTrail Eventi Insights	`Insight`	Questo tipo di archivio dati di eventi può raccogliere eventi CloudTrail Insights. Per ricevere eventi Insights, è necessario un archivio dati di origine degli eventi che registri gli eventi di CloudTrail gestione e abiliti Insights. Per informazioni sulla creazione degli archivi dati degli eventi di origine e di destinazione, consulta Creare un data store di eventi per gli eventi CloudTrail Insights.
Elementi di configurazione	`ConfigurationItem`	Questo tipo di archivio dati di eventi può raccogliere elementi AWS Config di configurazione. Per ulteriori informazioni, consulta Creare un archivio dati di eventi per gli elementi AWS Config di configurazione.
Eventi dall'integrazione	`ActivityAuditLog`	Questo tipo di archivio dati di eventi può raccogliere AWS eventi diversi dalle integrazioni. Per ulteriori informazioni, consulta Creare un archivio dati di AWS eventi per eventi esterni a.

È inoltre possibile creare un archivio dati di eventi per AWS Audit Manager le prove utilizzando la console Audit Manager. Per ulteriori informazioni sull'aggregazione delle prove in CloudTrail Lake

utilizzando Audit Manager, consulta Comprendere come funziona Evidence Finder con CloudTrail Lake nella Guida per l'AWS Audit Manager utente.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Le sezioni seguenti descrivono come creare, aggiornare e gestire gli archivi dati degli eventi.

Argomenti

- Crea, aggiorna e gestisci gli archivi dati degli eventi con la console
- Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI
- Gestione dei cicli di vita dell'archivio di dati degli eventi
- Copia di eventi traccia in un archivio dati degli eventi
- Federare un datastore di eventi
- Comprendere gli archivi di dati degli eventi organizzativi

Crea, aggiorna e gestisci gli archivi dati degli eventi con la console

È possibile utilizzare la CloudTrail console per creare, aggiornare, eliminare e ripristinare archivi di dati di eventi.

È possibile aggiornare le seguenti impostazioni utilizzando la CloudTrail console:

- Puoi modificare l'opzione di prezzo da un prezzo di fidelizzazione di sette anni a un prezzo di fidelizzazione estendibile per un anno.
- È possibile aggiornare il periodo di conservazione per l'archivio dati degli eventi. Il periodo di conservazione determina la durata di conservazione dei dati degli eventi presenti nel datastore di eventi.
- È possibile convertire un Data Store di eventi con più aree geografiche in un Data Store di eventi con un'unica area oppure convertire un Data Store di eventi con una singola area in un Data Store di eventi con più aree geografiche.
- L'account di gestione di un' AWS Organizations organizzazione può convertire un data store di eventi a livello di account in un data store di eventi organizzativi oppure può convertire un

data store di eventi dell'organizzazione in un data store di eventi a livello di account. Questa impostazione non è disponibile negli archivi dati di eventi che raccolgono eventi esterni a. AWS

- È possibile abilitare o disabilitare la federazione delle query di Lake. La federazione di un data store di eventi ti consente di interrogare i dati degli eventi da Amazon Athena.
- Puoi aggiungere o modificare la politica basata sulle risorse per un data store di eventi per fornire l'accesso a più account al tuo data store di eventi. Per ulteriori informazioni, consulta Esempi di policy basate su risorse per archivi di dati di eventi.
- È possibile interrompere l'acquisizione di eventi e riavviare l'acquisizione di eventi negli archivi di dati di eventi che raccolgono eventi di gestione, eventi di dati o elementi di configurazione. AWS Config
- È possibile abilitare o disabilitare la protezione dalla terminazione. L'attivazione della protezione dalla terminazione protegge un Event Data Store dall'eliminazione accidentale. La protezione dalla terminazione è abilitata per impostazione predefinita.
- È possibile ripristinare un archivio dati di eventi in attesa di eliminazione.
- È possibile aggiungere o rimuovere tag. Puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso al datastore di eventi.
- È possibile aggiungere una chiave KMS per crittografare il data store degli eventi. Non puoi rimuovere una chiave KMS da un archivio dati di eventi.

L'utilizzo della CloudTrail console per creare o aggiornare un archivio dati di eventi offre i seguenti vantaggi:

- Se stai configurando un data store di eventi per raccogliere eventi di dati, l'utilizzo della CloudTrail console ti consente di visualizzare i tipi di risorse di eventi di dati disponibili. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.
- Se stai configurando un Event Data Store per raccogliere eventi di attività di rete, l'utilizzo della CloudTrail console ti consente di visualizzare le fonti di eventi per le quali puoi registrare gli eventi di attività di rete. Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.
- Se stai configurando un Event Data Store per raccogliere eventi all'esterno AWS, l'utilizzo della CloudTrail console ti consente di visualizzare informazioni sui partner disponibili. Per ulteriori informazioni, consulta Crea un archivio dati di eventi per eventi esterni AWS alla console.

Argomenti

- Crea un archivio dati di CloudTrail eventi per gli eventi con la console

- Crea un archivio dati sugli eventi per gli eventi Insights con la console
- Crea un archivio dati di eventi per gli elementi di configurazione con la console
- Crea un archivio dati di eventi per eventi esterni AWS alla console
- Aggiorna un data store di eventi con la console
- Interrompi e avvia l'acquisizione di eventi con la console
- Modificare la protezione dalla terminazione con la console
- Eliminare un archivio dati di eventi con la console
- Ripristina un archivio dati di eventi con la console

Crea un archivio dati di CloudTrail eventi per gli eventi con la console

Gli archivi dati CloudTrail sugli eventi possono includere eventi di CloudTrail gestione, eventi di dati ed eventi di attività di rete. Puoi conservare i dati degli eventi in un datastore di eventi per un massimo di 3.653 giorni (circa 10 anni) se scegli l'opzione Prezzo per la conservazione estendibile di un anno o di 2.557 giorni (circa 7 anni) se scegli l'opzione Prezzo per la conservazione di sette anni.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Per creare un archivio dati per CloudTrail gli eventi

Utilizzare questa procedura per creare un archivio dati di eventi che registri gli eventi di CloudTrail gestione, gli eventi relativi ai dati o gli eventi di attività di rete.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configure event data store (Configura archivio di dati degli eventi), in General details (Dettagli generali), inserire un nome per l'archivio di dati degli eventi. Il nome è obbligatorio.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di

conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

Sono disponibili le seguenti opzioni:

- Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita.
  - Periodo di conservazione predefinito: 366 giorni
  - Periodo di conservazione massimo: 3.653 giorni
- Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
  - Periodo di conservazione predefinito: 2.557 giorni
  - Periodo di conservazione massimo: 2.557 giorni

6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

   CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

   > **Note**
   >
   > Se stai copiando eventi di trail in questo event data store, non CloudTrail copierà un evento se `eventTime` è più vecchio del periodo di conservazione specificato. Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'archivio dati degli eventi (periodo di conservazione = *`oldest-event-in-days`* +*`number-days-to-retain`*). Ad esempio, se l'evento più vecchio da copiare

risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.

7. (Facoltativo) Per abilitare l'utilizzo della crittografia AWS Key Management Service, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno per te, oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/ MyAliasName` L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia dell'archivio dati degli eventi. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

   L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

   > **Note**
   >
   > Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.

   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.

c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) Nella sezione Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso alil datastore di eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai

tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.

11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Scegli eventi, scegli AWS gli eventi, quindi scegli CloudTrail gli eventi.
13. Per CloudTrail gli eventi, scegli almeno un tipo di evento. Per impostazione predefinita è selezionato il tipo Management events (Eventi di gestione). Puoi aggiungere eventi di gestione, eventi relativi ai dati ed eventi di attività di rete al tuo archivio dati di eventi.
14. (Opzionale) Scegli Copia eventi di percorso se si desidera copiare gli eventi da un percorso esistente per eseguire query su eventi passati. Per copiare gli eventi del trail in un datastore di eventi dell'organizzazione, devi utilizzare l'account di gestione dell'organizzazione. L'account dell'amministratore delegato non può copiare gli eventi di trail in un datastore di eventi di un'organizzazione. Per ulteriori informazioni sulle considerazioni per la copia di eventi di percorso, consulta Considerazioni sulla copia di eventi di percorso.
15. Per fare in modo che il proprio archivio di dati degli eventi raccolga eventi da tutti gli account in un'organizzazione AWS Organizations , selezionare Enable for all accounts in my organization (Abilita per tutti gli account nella mia organizzazione). Per creare un datastore di eventi che raccolga gli eventi per un'organizzazione, è necessario effettuare l'accesso all'account di gestione o all'account dell'amministratore delegato di un'organizzazione.

> **Note**
>
> Per copiare gli eventi di percorso o abilitare gli eventi Insights, è necessario accedere all'account di gestione dell'organizzazione.

16. Espandi Impostazioni aggiuntive per scegliere se desideri che il tuo Event Data Store raccolga gli eventi per tutti Regioni AWS o solo per quelli correnti Regione AWS e scegli se l'Event Data Store inserisce gli eventi. Per impostazione predefinita, un datastore di eventi raccoglie eventi da tutte le Regioni e inizia a importarli al momento della creazione.

    a. Seleziona Includi solo la Regione corrente nel mio datastore di eventi per includere solo gli eventi registrati nella Regione corrente. Se non si sceglie questa opzione, l'archivio di dati degli eventi include gli eventi provenienti da tutte le regioni.

    b. Deseleziona l'opzione Eventi di importazione se non desideri che il datastore di eventi inizi a importare gli eventi. Ad esempio, potresti voler deselezionare Eventi di importazione, se stai copiando gli eventi di percorso e non desideri che il datastore di eventi includa eventi

futuri. Per impostazione predefinita, il datastore di eventi inizia l'importazione degli eventi al momento della creazione.

17. Se il tuo datastore di eventi include eventi di gestione, puoi scegliere tra le seguenti opzioni. Per ulteriori informazioni sugli eventi di gestione, consulta Registrazione degli eventi di gestione.

    a. Scegli tra Raccolta di eventi semplice o Raccolta di eventi avanzata:

        - Scegli Simple event collection se desideri registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere AWS Key Management Service eventi Amazon RDS Data API.
        - Scegli Advanced event collection se desideri includere o escludere eventi di gestione in base ai valori dei campi avanzati di selezione degli eventi, inclusi i campi`eventName`,`eventType`, `eventSourcesessionCredentialFromConsole`, `euserIdentity.arn`.

    b. Se hai selezionato Raccolta di eventi semplice, scegli se registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere AWS KMS eventi Amazon RDS Data API.

    c. Se hai selezionato Raccolta eventi avanzata, effettua le seguenti selezioni:

        i. In Log selector template, scegli un modello predefinito o Personalizzato per creare una configurazione personalizzata basata sui valori avanzati dei campi del selettore di eventi.

            Puoi scegliere tra i seguenti modelli predefiniti:

            - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
            - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
            - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
            - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console

- Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

ii. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio «Registra gli eventi di gestione delle sessioni». AWS Management Console Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

iii. Se hai scelto Personalizzato, in Advanced event selectors crea un'espressione basata sui valori avanzati dei campi del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

A. Scegli tra i seguenti campi.

- **`readOnly`**— `readOnly` può essere impostato in modo che sia uguale a un valore di o. `true` `false` Quando è impostato su`false`, l'Event Data Store registra gli eventi di gestione di sola scrittura. Gli eventi di gestione di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi or. `Get*` `Describe*` Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia gli eventi di lettura che quelli di scrittura, non aggiungete un `readOnly` selettore.
- **`eventName`**— `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento di gestione, ad esempio `CreateAccessPoint` o`GetAccessPoint`.
- **`userIdentity.arn`**— Includi o escludi eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .

- **`sessionCredentialFromConsole`**— Includi o escludi eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- **`eventSource`**— È possibile utilizzarlo per includere o escludere fonti di eventi specifiche. In genere `eventSource` è una forma abbreviata del nome del servizio senza spazi plus `.amazonaws.com`. Ad esempio, puoi impostare `eventSource` equals to per registrare solo gli `ec2.amazonaws.com` eventi di EC2 gestione di Amazon.
- **`eventType`**— L'EventType da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale per escludere **`AwsServiceEvent`** gli eventi.Servizio AWS

B. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

Per informazioni su come CloudTrail valuta più condizioni, vedere. Come CloudTrail valuta più condizioni per un campo

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

C. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

iv. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

d. Scegli Abilita l'acquisizione degli eventi di Insights per abilitare Insights. Per abilitare Insights, è necessario configurare un datastore di eventi di destinazione per raccogliere gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi.

Se scegli di abilitare Insights, procedi come segue.

i. Scegli l'archivio eventi di destinazione che registrerà gli eventi di Insights. Il datastore di eventi di destinazione raccoglierà gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi. Per informazioni su come creare il datastore di

eventi di destinazione, consulta Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights.

ii. Scegli i tipi di Insights. Puoi scegliere la frequenza delle chiamate API, la frequenza di errore API o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.

18. Per includere gli eventi di dati nell'archivio di dati degli eventi, procedere come segue.

    a. Scegli un tipo di risorsa. Questa è la risorsa Servizio AWS e su cui vengono registrati gli eventi relativi ai dati.

    b. Nel modello di selettore di registro, scegli un modello predefinito o scegli Personalizzato per definire le tue condizioni di raccolta degli eventi in base ai valori dei campi avanzati del selettore di eventi.

       Puoi scegliere tra i seguenti modelli predefiniti:

       - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
       - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
       - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
       - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
       - Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

    c. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

    d. Se hai selezionato Personalizzato, in Advanced event selector crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

i. Scegli tra i seguenti campi.

- **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.
- **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`
- **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.
- eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete
- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.`ARN, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.ARN` campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere gli eventi di dati per due bucket S3 dagli eventi di dati registrati nel tuo event data store, puoi impostare il campo su Resources.arn, impostare l'operatore for does not start con e quindi incollare un bucket S3 ARN per il quale non desideri registrare gli eventi.

Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

e. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

f. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati. Ripeti i passaggi da 1 a questo passaggio per configurare i selettori di eventi avanzati per il tipo di risorsa.

19. Per includere gli eventi relativi alle attività di rete nel tuo archivio dati degli eventi, procedi come segue.

    a. Da Origine eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.

    b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.

    c. (Facoltativo) Inserisci un nome per identificare il selettore. Il nome del selettore è elencato come Nome nel selettore di eventi avanzato ed è visualizzabile se si espande la vista JSON.

    d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

        i. Per escludere o includere gli eventi di attività di rete, puoi scegliere tra i seguenti campi nella console.

            - **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi usarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
            - **`errorCode`**— È possibile utilizzarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.
            - **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

        ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

        iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

    e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

    f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

20. Per copiare gli eventi di trail nel datastore di eventi, esegui la seguente procedura.

a. Scegliere il percorso che si vuole copiare. Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel prefisso del bucket S3 e i `CloudTrail` prefissi all'interno del prefisso e non controlla i `CloudTrail` prefissi per altri servizi. AWS Se desideri copiare gli CloudTrail eventi contenuti in un altro prefisso, scegli Inserisci URI S3, quindi scegli Browse S3 per cercare il prefisso. Se il bucket S3 di origine per il percorso utilizza una chiave KMS per la crittografia dei dati, assicurati che la politica della chiave KMS consenta di decrittografare i dati. CloudTrail Se il tuo bucket S3 di origine utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail Per ulteriori informazioni sull'aggiornamento della policy delle chiavi KMS, consulta Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine.

b. Scegli l'intervallo di tempo per copiare gli eventi. CloudTrail controlla il prefisso e il nome del file di registro per verificare che il nome contenga una data compresa tra la data di inizio e di fine scelte prima di tentare di copiare gli eventi del trail. Puoi scegliere un Intervallo relativo o un Intervallo assoluto. Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, scegliere un intervallo di tempo antecedente alla creazione dell'archivio dati degli eventi.

> **Note**
>
> CloudTrail copia solo gli eventi di trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Ad esempio, se il periodo di conservazione di un Event Data Store è di 90 giorni, non CloudTrail copierà alcun evento di trail con una data `eventTime` più vecchia di 90 giorni.

- Se scegli Intervallo relativo, puoi scegliere di copiare gli eventi registrati negli ultimi 6 mesi, 1 anno, 2 anni, 7 anni o un intervallo personalizzato. CloudTrail copia gli eventi registrati nel periodo di tempo scelto.
- Se scegli l'intervallo assoluto, puoi scegliere una data di inizio e di fine specifica. CloudTrail copia gli eventi che si sono verificati tra le date di inizio e di fine scelte.

c. Per Autorizzazioni, scegli una delle opzioni seguenti del ruolo IAM. Se scegli un ruolo IAM esistente, accertati che la policy dei ruoli IAM fornisca le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiornamento delle autorizzazioni del ruolo IAM, consultare Autorizzazioni IAM per la copia di eventi traccia

- Scegli Creare un nuovo ruolo (consigliato) per creare un nuovo ruolo IAM. Per Inserisci il nome del ruolo IAM, inserisci un nome per il ruolo. CloudTrail crea automaticamente le autorizzazioni necessarie per questo nuovo ruolo.
- Scegli Usa un ruolo IAM personalizzato ARN per utilizzare un ruolo IAM personalizzato non elencato. Per Inserisci ARN ruolo IAM, inserisci l'ARN IAM.
- Scegli un ruolo IAM esistente dall'elenco a discesa.

21. Scegli Avanti per arricchire i tuoi eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.
22. In Enrich events, aggiungi fino a 50 chiavi di tag di risorsa e 50 chiavi di condizione globali IAM per fornire metadati aggiuntivi sui tuoi eventi. Questo ti aiuta a classificare e raggruppare gli eventi correlati.

    Se aggiungi chiavi di tag di risorsa, CloudTrail includerà le chiavi di tag selezionate associate alle risorse coinvolte nella chiamata API. Gli eventi API relativi alle risorse eliminate non avranno tag di risorsa.

    Se aggiungi chiavi di condizione globali IAM, CloudTrail includerà informazioni sulle chiavi di condizione selezionate che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione, sulla rete e sulla richiesta stessa.

    Le informazioni sulle chiavi dei tag di risorsa e sulle chiavi di condizione globali IAM sono mostrate nel `eventContext` campo dell'evento. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.

    > **Note**
    >
    > Se un evento contiene una risorsa che non appartiene alla regione dell'evento, non CloudTrail compilerà i tag per questa risorsa perché il recupero dei tag è limitato alla regione dell'evento.

23. Scegliete Espandi la dimensione dell'evento per espandere il payload dell'evento fino a 1 MB da 256 KB. Questa opzione viene abilitata automaticamente quando aggiungi chiavi di tag di risorsa o chiavi di condizione globale IAM per garantire che tutte le chiavi aggiunte siano incluse nell'evento.

L'espansione della dimensione dell'evento è utile per l'analisi e la risoluzione dei problemi degli eventi, poiché consente di visualizzare l'intero contenuto dei seguenti campi, purché il payload dell'evento sia inferiore a 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Per ulteriori informazioni su questi campi, consulta il contenuto dei CloudTrail record.

24. Scegli Next (Successivo) per rivedere le scelte effettuate.
25. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
26. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.

    Da questo momento in poi, il datastore di eventi catturerà gli eventi che corrispondono ai suoi selettori di eventi avanzati (se mantieni l'opzione Eventi di importazione selezionata). Gli eventi che si sono verificati prima della creazione dell'archivio di dati degli eventi non si trovano all'interno dell'archivio, a meno che tu non si abbia scelto di copiare gli eventi di trail esistenti.

Ora è possibile eseguire query sul nuovo datastore di eventi. La scheda Sample queries (Query di esempio) fornisce query di esempio per iniziare. Per ulteriori informazioni sulla creazione e la modifica di query, consulta Crea o modifica un'interrogazione con la console CloudTrail .

Puoi anche visualizzare le dashboard gestite o creare dashboard personalizzate per visualizzare le tendenze degli eventi. Per ulteriori informazioni sui pannelli di controllo di Lake, consulta CloudTrail Cruscotti Lake.

Crea un archivio dati sugli eventi per gli eventi Insights con la console

AWS CloudTrail Insights aiuta AWS gli utenti a identificare e rispondere alle attività insolite associate ai tassi di chiamata e ai tassi di errore delle API analizzando continuamente gli eventi di CloudTrail gestione. CloudTrail Insights analizza i normali modelli di frequenza delle chiamate e dei tassi di errore delle API, detti anche baseline, e genera eventi Insights quando il volume delle chiamate o i tassi di errore non rientrano negli schemi normali. Gli eventi Insights sulla frequenza delle chiamate API vengono generati per la `write` gestione APIs, mentre gli eventi Insights sul tasso di errore delle API vengono generati sia per la gestione che per `read` la `write` gestione APIs.

Per registrare gli eventi di Insights in CloudTrail Lake, è necessario un data store di eventi di destinazione che registri gli eventi di Insights e un data store di eventi di origine che abiliti Insights e registri gli eventi di gestione.

> **Note**
>
> Per registrare gli eventi di Insights sulla frequenza delle chiamate API, il data store degli eventi di origine deve registrare gli eventi di `write` gestione. Per registrare gli eventi di Insights sul tasso di errore dell'API, l'archivio dati degli eventi di origine deve registrare `read` o `write` gestire gli eventi.

Se hai abilitato CloudTrail Insights su un data store di eventi di origine e CloudTrail rileva attività insolite, CloudTrail invia gli eventi Insights al data store degli eventi di destinazione. A differenza di altri tipi di eventi acquisiti in un archivio dati di CloudTrail eventi, gli eventi di Insights vengono registrati solo quando CloudTrail rileva cambiamenti nell'utilizzo dell'API dell'account che differiscono in modo significativo dai modelli di utilizzo tipici dell'account.

Dopo aver abilitato CloudTrail Insights per la prima volta su un Event Data Store, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi di Insights, a condizione che durante quel periodo venga rilevata un'attività insolita.

CloudTrail Insights analizza gli eventi di gestione che si verificano in ciascuna regione per il data store degli eventi e genera un evento Insights quando viene rilevata un'attività insolita che si discosta dalla linea di base. Un evento CloudTrail Insights viene generato nella stessa regione in cui viene generato l'evento di gestione di supporto.

Per un archivio dati di eventi organizzativi, CloudTrail Insights analizza gli eventi di gestione di ogni account membro dell'organizzazione per ogni regione e genera un evento Insights quando viene rilevata un'attività insolita che si discosta dalla linea di base per l'account e la regione.

Si applicano costi aggiuntivi per l'acquisizione di eventi Insights in Lake. CloudTrail L'addebito verrà effettuato separatamente se attivi Insights sia per i trail che per i data store di eventi CloudTrail Lake. Per informazioni sui CloudTrail prezzi, consulta AWS CloudTrail Prezzi.

Argomenti

- Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights
- Creazione di un datastore di eventi di origine che registra gli eventi di Insights

Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights

Quando si crea un datastore di eventi Insights, è possibile scegliere un datastore di eventi di origine esistente che registri gli eventi di gestione e quindi specificare i tipi di Insights che si desidera ricevere. In alternativa, puoi abilitare Insights su un datastore di eventi nuovo o esistente dopo aver creato il tuo datastore di eventi di Insights e quindi scegliere questo datastore come datastore di eventi di destinazione.

Questa procedura mostra come creare un datastore di eventi di destinazione che registra gli eventi di Insights.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, apri il sottomenu Lake, quindi scegli Event data stores (Archivi di dati degli eventi).
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configure event data store (Configura archivio di dati degli eventi), in General details (Dettagli generali), inserire un nome per l'archivio di dati degli eventi. Il nome è obbligatorio.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

- Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita.
  - Periodo di conservazione predefinito: 366 giorni
  - Periodo di conservazione massimo: 3.653 giorni
- Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
  - Periodo di conservazione predefinito: 2.557 giorni
  - Periodo di conservazione massimo: 2.557 giorni

6. Specificare un periodo di conservazione per l'archivio di dati degli eventi espresso in giorni. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni. L'archivio di dati degli eventi conserva i dati degli eventi per il numero specificato di giorni.
7. (Facoltativo) Per abilitare l'utilizzo della crittografia AWS Key Management Service, scegli Usa la mia. AWS KMS key Scegli Nuovo per AWS KMS key crearne uno per te, oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/` *`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia dell'archivio dati degli eventi. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

   L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

> **Note**
>
> Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.
   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.
   c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`

- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) Nella sezione Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso alil datastore di eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.
11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Scegli eventi, scegli gli AWS eventi, quindi scegli gli eventi di CloudTrailInsights.
13. Negli eventi CloudTrail Insights, procedi come segue.

    a. Scegli Consenti l'accesso come amministratore delegato se desideri concedere all'amministratore delegato della tua organizzazione l'accesso a questo datastore di eventi. Questa opzione è disponibile solo se hai effettuato l'accesso con l'account di gestione di un' AWS Organizations organizzazione.

    b. (Facoltativo) Scegli un datastore di eventi di origine esistente che registri gli eventi di gestione e specifica i tipi di Insights che desideri ricevere.

       Per aggiungere un datastore di eventi di origine, procedere come segue.

       i. Scegli Aggiungi datastore di eventi di origine.

ii. Scegli il datastore di eventi di origine.

iii. Scegli il tipo di Insights che desideri ricevere.

- `ApiCallRateInsight`: il tipo di Insights `ApiCallRateInsight` analizza le chiamate API di gestione in sola scrittura aggregate al minuto rispetto a un volume di chiamate API di base. Per ricevere Insights su `ApiCallRateInsight`, il datastore di eventi di origine deve registrare gli eventi di gestione Write.
- `ApiErrorRateInsight`: il tipo di Insights `ApiErrorRateInsight` analizza le chiamate API di gestione che generano codici di errore. L'errore viene visualizzato se la chiamata API non ha esito positivo. Per ricevere Insights su `ApiErrorRateInsight`, il datastore di eventi di origine deve registrare gli eventi di gestione Write o Read.

iv. Ripeti i due passaggi precedenti (ii e iii) per aggiungere eventuali altri tipi di Insights che desideri ricevere.

14. Scegli Next (Successivo) per rivedere le scelte effettuate.
15. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
16. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.
17. Se non hai scelto un datastore di eventi di origine nel passaggio 10, segui la procedura riportata in Creazione di un datastore di eventi di origine che registra gli eventi di Insights per creare un datastore di eventi di origine.

Creazione di un datastore di eventi di origine che registra gli eventi di Insights

Questa procedura mostra come creare un datastore di eventi di origine che abilita gli eventi Insights e registra gli eventi di gestione.

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, apri il sottomenu Lake, quindi scegli Event data stores (Archivi di dati degli eventi).
3. Scegliere Create event data store (Crea archivio di dati degli eventi).

4. Nella pagina Configure event data store (Configura archivio di dati degli eventi), in General details (Dettagli generali), inserire un nome per l'archivio di dati degli eventi. Il nome è obbligatorio.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

   - Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita.
     - Periodo di conservazione predefinito: 366 giorni
     - Periodo di conservazione massimo: 3.653 giorni
   - Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
     - Periodo di conservazione predefinito: 2.557 giorni
     - Periodo di conservazione massimo: 2.557 giorni
6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

   CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.
7. (Facoltativo) Per abilitare l'utilizzo della crittografia AWS Key Management Service, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno per te, oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/` *`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica

delle chiavi KMS per consentire la crittografia e la decrittografia dell'archivio dati degli eventi. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

> **Note**
>
> Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.

   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.

   c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di

interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) Nella sezione Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso alil datastore di eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.
11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Scegli eventi, scegli AWS gli eventi, quindi scegli CloudTrail gli eventi.
13. Negli CloudTrail eventi, lascia selezionata l'opzione Eventi di gestione.

14. Per fare in modo che il proprio archivio di dati degli eventi raccolga eventi da tutti gli account in un'organizzazione AWS Organizations , selezionare Enable for all accounts in my organization (Abilita per tutti gli account nella mia organizzazione). Per creare un datastore di eventi che abiliti Insights, è necessario effettuare l'accesso all'account di gestione dell'organizzazione.
15. Espandi Impostazioni aggiuntive per scegliere se desideri che il tuo Event Data Store raccolga gli eventi per tutti Regioni AWS o solo per quelli correnti Regione AWS e scegli se il Data Store degli eventi inserisce gli eventi. Per impostazione predefinita, un datastore di eventi raccoglie eventi da tutte le Regioni e inizia a importarli al momento della creazione.
    a. Se desideri includere solo gli eventi che sono registrati nella Regione corrente, seleziona Includi solo la Regione corrente nel mio datastore di eventi. Se non si sceglie questa opzione, l'archivio di dati degli eventi include gli eventi provenienti da tutte le regioni.
    b. Lascia selezionata l'opzione Eventi di importazione.
16. Scegli tra Raccolta di eventi semplice o Raccolta di eventi avanzata:
    - Scegli Simple event collection se desideri registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere AWS Key Management Service eventi Amazon RDS Data API.
    - Scegli Advanced event collection se desideri includere o escludere eventi di gestione in base ai valori dei campi avanzati di selezione degli eventi, inclusi i campi`eventName`,`eventType`, `eventSourcesessionCredentialFromConsole`, `euserIdentity.arn`.
17. Se hai selezionato Raccolta di eventi semplice, scegli se registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere AWS KMS eventi Amazon RDS Data API.
18. Se hai selezionato Raccolta eventi avanzata, effettua le seguenti selezioni:
    a. Nel modello di selettore di registro, scegli un modello predefinito o scegli Personalizzato per scrivere le tue condizioni di raccolta degli eventi in base ai valori dei campi avanzati del selettore di eventi.

       Puoi scegliere tra i seguenti modelli predefiniti:

       - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
       - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.

- Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
- Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
- Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

b. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio «Registra gli eventi di gestione delle sessioni». AWS Management Console Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

c. Se hai scelto Personalizzato, in Advanced event selectors crea un'espressione basata sui valori avanzati dei campi del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

i. Scegli tra i seguenti campi.

- **`readOnly`**— `readOnly` può essere impostato in modo che sia uguale a un valore di o. `true` `false` Quando è impostato su`false`, l'Event Data Store registra gli eventi di gestione di sola scrittura. Gli eventi di gestione di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi or. `Get*` `Describe*` Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia gli eventi di lettura che quelli di scrittura, non aggiungete un `readOnly` selettore.
- **`eventName`**— `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento di gestione, ad esempio `CreateAccessPoint` o`GetAccessPoint`.

- **`userIdentity.arn`**— Includi o escludi eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`sessionCredentialFromConsole`**— Includi o escludi eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- **`eventSource`**— È possibile utilizzarlo per includere o escludere fonti di eventi specifiche. In genere `eventSource` è una forma abbreviata del nome del servizio senza spazi plus `.amazonaws.com`. Ad esempio, puoi impostare `eventSource` equals to per registrare solo gli `ec2.amazonaws.com` eventi di EC2 gestione di Amazon.
- **`eventType`**— L'EventType da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale per escludere **`AwsServiceEvent`** gli eventi.Servizio AWS

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

Per informazioni su come CloudTrail valuta più condizioni, vedere. Come CloudTrail valuta più condizioni per un campo

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

d. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

19. Scegli Abilita l'acquisizione degli eventi di Insights.
20. Scegli l'archivio eventi di destinazione che registrerà gli eventi di Insights. Il datastore di eventi di destinazione raccoglierà gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi. Per informazioni su come creare il datastore di eventi di destinazione, consulta Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights.

21. Scegli i tipi di Insights. Puoi scegliere la frequenza delle chiamate API, la frequenza di errore API o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.
22. Scegli Avanti per arricchire i tuoi eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.
23. In Enrich events, aggiungi fino a 50 chiavi di tag di risorsa e 50 chiavi di condizione globali IAM per fornire metadati aggiuntivi sui tuoi eventi. Questo ti aiuta a classificare e raggruppare gli eventi correlati.

    Se aggiungi chiavi di tag di risorsa, CloudTrail includerà le chiavi di tag selezionate associate alle risorse coinvolte nella chiamata API. Gli eventi API relativi alle risorse eliminate non avranno tag di risorsa.

    Se aggiungi chiavi di condizione globali IAM, CloudTrail includerà informazioni sulle chiavi di condizione selezionate che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione, sulla rete e sulla richiesta stessa.

    Le informazioni sulle chiavi dei tag di risorsa e sulle chiavi di condizione globali IAM sono mostrate nel `eventContext` campo dell'evento. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.

    > **Note**
    >
    > Se un evento contiene una risorsa che non appartiene alla regione dell'evento, non CloudTrail compilerà i tag per questa risorsa perché il recupero dei tag è limitato alla regione dell'evento.

24. Scegliete Espandi la dimensione dell'evento per espandere il payload dell'evento fino a 1 MB da 256 KB. Questa opzione viene abilitata automaticamente quando aggiungi chiavi di tag di risorsa o chiavi di condizione globale IAM per garantire che tutte le chiavi aggiunte siano incluse nell'evento.

    L'espansione della dimensione dell'evento è utile per l'analisi e la risoluzione dei problemi degli eventi, poiché consente di visualizzare l'intero contenuto dei seguenti campi, purché il payload dell'evento sia inferiore a 1 MB:

    - `annotation`

- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Per ulteriori informazioni su questi campi, consulta il contenuto dei CloudTrail record.

25. Scegli Next (Successivo) per rivedere le scelte effettuate.
26. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
27. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.

    Da questo momento in poi, l'archivio di dati degli eventi cattura gli eventi che corrispondono ai suoi selettori di eventi avanzati. Dopo aver abilitato CloudTrail Insights per la prima volta nel tuo archivio dati di origine degli eventi, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi di Insights, a condizione che venga rilevata un'attività insolita durante quel periodo.

    Puoi visualizzare la dashboard di CloudTrail Lake per visualizzare gli eventi Insights nel data store degli eventi di destinazione. Per ulteriori informazioni sui pannelli di controllo di Lake, consulta CloudTrail Cruscotti Lake.

Si applicano costi aggiuntivi per l'acquisizione di eventi Insights in Lake. CloudTrail Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Crea un archivio dati di eventi per gli elementi di configurazione con la console

Puoi creare un datastore di eventi per includere gli elementi di configurazione AWS Config e utilizzarlo per esaminare le modifiche non conformi agli ambienti di produzione. Con un datastore

di eventi, puoi mettere in relazione le regole non conformi con gli utenti e le risorse associati alle modifiche. Un elemento di configurazione rappresenta una point-in-time visualizzazione degli attributi di una AWS risorsa supportata presente nell'account. AWS Config crea un elemento di configurazione ogni volta che rileva una modifica a un tipo di risorsa che sta registrando. AWS Config crea inoltre elementi di configurazione quando viene acquisita un'istantanea di configurazione.

Puoi usare entrambi AWS Config e CloudTrail Lake per eseguire query sugli elementi di configurazione. È possibile utilizzare AWS Config per interrogare lo stato di configurazione corrente delle AWS risorse in base alle proprietà di configurazione per un singolo account Account AWS e Regione AWS regioni o per più account e regioni. Al contrario, puoi usare CloudTrail Lake per eseguire query su diverse fonti di dati come CloudTrail eventi, elementi di configurazione e valutazioni delle regole. CloudTrail Le query di Lake coprono tutti gli elementi AWS Config di configurazione, inclusa la configurazione delle risorse e la cronologia della conformità.

La creazione di un archivio dati di eventi per gli elementi di configurazione non ha alcun impatto sulle query AWS Config avanzate esistenti o sugli aggregatori configurati AWS Config . Puoi continuare a eseguire query avanzate utilizzando AWS Config e AWS Config continuare a fornire file di cronologia ai tuoi bucket S3.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Limitazioni

Le seguenti limitazioni si applicano ai datastore di eventiper gli elementi di configurazione.

- Nessun supporto per elementi di configurazione personalizzati
- Nessun supporto per il filtro degli eventi tramite selettori di eventi avanzati

Prerequisiti

Prima di creare il tuo archivio dati sugli eventi, configura AWS Config la registrazione per tutti i tuoi account e le tue regioni. Puoi utilizzare Quick Setup, una funzionalità di AWS Systems Manager, per creare rapidamente un registratore di AWS Config configurazione basato su.

> **Note**
>
> All' AWS Config avvio della registrazione delle configurazioni vengono addebitati i costi di utilizzo del servizio. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS Config. Per ulteriori informazioni sulla gestione del registratore di configurazione, consulta Gestione del registratore della configurazione nella Guida per gli sviluppatori di AWS Config .

Inoltre, le seguenti azioni sono consigliate, ma non obbligatorie per creare un datastore di eventi.

- Configura un bucket Amazon S3 per ricevere uno snapshot di configurazione su richiesta e la cronologia di configurazione. Per ulteriori informazioni sugli snapshot, consulta Managing the Delivery Channel (Gestione del canale di distribuzione) e Delivering Configuration Snapshot to an Amazon S3 Bucket (Distribuzione dello snapshot di configurazione in un bucket Amazon S3) nella Guida per gli sviluppatori di AWS Config .
- Specificate le regole che desiderate utilizzare AWS Config per valutare le informazioni di conformità per i tipi di risorse registrati. Alcune delle query di esempio di CloudTrail Lake AWS Config richiedono Regole di AWS Config la valutazione dello stato di conformità delle AWS risorse. Per ulteriori informazioni in merito Regole di AWS Config, consulta Evaluating Resources with Regole di AWS Config nella AWS Config Developer Guide.

Creazione di un datastore di eventi per gli elementi di configurazione

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configure event data store (Configura archivio di dati degli eventi), in General details (Dettagli generali), inserire un nome per l'archivio di dati degli eventi. Il nome è obbligatorio.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

- Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita.
  - Periodo di conservazione predefinito: 366 giorni
  - Periodo di conservazione massimo: 3.653 giorni
- Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
  - Periodo di conservazione predefinito: 2.557 giorni
  - Periodo di conservazione massimo: 2.557 giorni

6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

   CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

7. (Facoltativo) Per abilitare l'utilizzo della crittografia AWS Key Management Service, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno per te, oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/` *`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia dell'archivio dati degli eventi. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

   L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

> **Note**
>
> Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.
   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.
   c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`

- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) Nella sezione Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso alil datastore di eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.
11. Scegli Next (Successivo).
12. Nella pagina Scegli eventi, scegli Eventi AWS , quindi seleziona Elementi di configurazione.
13. CloudTrail archivia la risorsa Event Data Store nella regione in cui è stata creata, ma per impostazione predefinita, gli elementi di configurazione raccolti nel data store provengono da tutte le regioni dell'account in cui è abilitata la registrazione. Se lo desideri, puoi selezionare Include only the current region in my event data store (Includi solo la regione corrente nel datastore di eventi) per includere solo gli eventi acquisiti nella regione corrente. Se non scegli questa opzione, il datastore di eventi include gli elementi di configurazione provenienti da tutte le regioni in cui è abilitata la registrazione.
14. Per fare in modo che il tuo Event Data Store raccolga gli elementi di configurazione da tutti gli account di un' AWS Organizations organizzazione, seleziona Abilita per tutti gli account della mia organizzazione. Per creare un datastore di eventi che raccolga gli elementi di configurazione

per un'organizzazione, è necessario effettuare l'accesso all'account di gestione o all'account dell'amministratore delegato dell'organizzazione stessa.

15. Scegli Next (Successivo) per rivedere le scelte effettuate.
16. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
17. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.

    Da questo momento in poi, il datastore di eventi registra gli elementi di configurazione. Gli elementi di configurazione che si sono verificati prima della creazione delil datastore di eventi non si trovano al suo interno.

Schema dell'elemento di configurazione

La tabella seguente descrive gli elementi dello schema obbligatori e facoltativi che corrispondono a quelli nei record degli elementi di configurazione. Il contenuto di `eventData` è fornito dagli elementi di configurazione; gli altri campi sono forniti da CloudTrail after ingestion.

CloudTrail i contenuti dei record di eventi sono descritti più dettagliatamente in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete

- Campi forniti da CloudTrail dopo l'ingestione
- Campi forniti dai tuoi eventi

Campi forniti da dopo l'ingestione CloudTrail

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
eventVersion	string	Richiesto	La versione del formato dell' AWS evento.
eventCategory	string	Richiesto	La categoria dell'even to. Per gli elementi di configurazione, il valore valido

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
			è `ConfigurationItem` .
eventType	string	Richiesto	Il tipo di evento, Per gli elementi di configurazione, il valore valido è `AwsConfigurationItem` .
eventID	string	Richiesto	Un ID univoco per un evento.
eventTime	string	Richiesto	Il timestamp dell'evento, in formato `yyyy-MM-DDTHH:mm:ss` Universal Coordinated Time (UTC).
awsRegion	string	Richiesto	Regione AWS A cui assegnare un evento.
recipientAccountId	string	Richiesto	Rappresenta l' Account AWS ID che ha ricevuto questo evento.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
addendum	addendum	Facoltativo	Mostra informazioni sul motivo per cui un evento è stato ritardato. Se mancavano informazioni da un evento esistente, il blocco aggiuntivo includerà le informazioni mancanti e un motivo per cui mancavano.

I campi in **`eventData`** sono forniti dagli elementi di configurazione

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
eventData	-	Richiesto	I campi in eventData sono forniti dagli elementi di configurazione
• configurationItemVersion	string	Facoltativo	La versione dell'elemento di configurazione dalla sua origine.
• configurationItemCaptureOra	string	Facoltativo	L'ora in cui è stata avviata la registrazione della configurazione.
• configurationItemStatus	string	Facoltativo	Lo stato dell'elemento di configurazione. I valori validi sono `OK`, `ResourceDiscovered`

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
			, `ResourceNotRecorded` , `ResourceDeleted` e `ResourceDeletedNotRecorded` .
• accountId	string	Facoltativo	L' Account AWS ID a 12 cifre associato alla risorsa.
• resourceType	string	Facoltativo	Il tipo di risorsa. AWS Per ulteriori informazioni sui tipi di risorse validi, Configurationitemconsulta l'AWS Config API Reference.
• resourceId	string	Facoltativo	L'ID della risorsa (ad esempio, sg-*xxxxxx*).
• resourceName	string	Facoltativo	Il nome personalizzato della risorsa, se disponibile.
• arn	string	Facoltativo	Il nome della risorsa Amazon (ARN) associato alla risorsa.
• awsRegion	string	Facoltativo	Il Regione AWS luogo in cui risiede la risorsa.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• availabilityZone	string	Facoltativo	La zona di disponibilità della risorsa associata alla risorsa.
• resourceCreationTime	string	Facoltativo	Il timestamp di quando è stata creata la risorsa.
• configurazione	JSON	Facoltativo	La descrizione della configurazione della risorsa.
• supplementaryConfiguration	JSON	Facoltativo	Attributi di configurazione AWS Config restituiti per determinati tipi di risorse per integrare le informazioni restituite per il parametro di configurazione.
• relatedEvents	string	Facoltativo	Un elenco di CloudTrail eventi IDs.
• relationships	-	Facoltativo	Un elenco di AWS risorse correlate.
• • nome	string	Facoltativo	Il tipo di relazione con la risorsa correlata.
• • resourceType	string	Facoltativo	Il tipo di risorsa della risorsa correlata.
• • resourceId	string	Facoltativo	L'ID della risorsa correlata (ad esempio, sg-*xxxxxx*).

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• • resourceName	string	Facoltativo	Il nome personalizzato della risorsa correlata, se disponibile.
• tags	JSON	Facoltativo	Una mappatura dei tag con i valori della chiave associati alla risorsa.

L'esempio seguente mostra la gerarchia di elementi dello schema che corrispondono a quelli nei record degli elementi di configurazione.

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
```

```
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

Crea un archivio dati di eventi per eventi esterni AWS alla console

Puoi creare un data store di AWS eventi per includere eventi esterni e quindi utilizzare CloudTrail Lake per cercare, interrogare e analizzare i dati registrati dalle tue applicazioni.

Puoi utilizzare le integrazioni di CloudTrail Lake per registrare e archiviare i dati sulle attività degli utenti dall'esterno AWS; da qualsiasi fonte nei tuoi ambienti ibridi, come applicazioni interne o SaaS ospitate in locale o nel cloud, macchine virtuali o contenitori.

Quando crei un archivio di dati degli eventi per un'integrazione, crei anche un canale e vi colleghi una policy delle risorse.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Per creare un archivio dati di eventi per eventi esterni a AWS

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configure event data store (Configura archivio di dati degli eventi), in General details (Dettagli generali), inserire un nome per l'archivio di dati degli eventi. Il nome è obbligatorio.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

   - Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a un pay-as-you-go prezzo. Questa è l'opzione predefinita.
     - Periodo di conservazione predefinito: 366 giorni
     - Periodo di conservazione massimo: 3.653 giorni
   - Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
     - Periodo di conservazione predefinito: 2.557 giorni
     - Periodo di conservazione massimo: 2.557 giorni
6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

   CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di

conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

7. (Facoltativo) Per abilitare l'utilizzo della crittografia AWS Key Management Service, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno per te, oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/` *`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia dell'archivio dati degli eventi. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

   L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

   > **Note**
   >
   > Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.

   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.

c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) Nella sezione Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso alil datastore di eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai

tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.

11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Choose events (Scegli eventi), scegli Events from integrations (Eventi dalle integrazioni).
13. Da Events from integration (Eventi dall'integrazione), scegli l'origine dalla quale distribuire gli eventi all'archivio di dati degli eventi.
14. Fornisci un nome per identificare il canale dell'integrazione. Il nome può contenere da 3 a 128 caratteri. Sono consentiti soltanto lettere, numeri, punti, e caratteri di sottolineatura e trattini.
15. In Resource policy (Policy delle risorse), configura la policy delle risorse per il canale dell'integrazione. Le policy delle risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un principale specificato sulla risorsa e in base a quali condizioni. Gli account definiti come principali nella policy delle risorse possono chiamare l'API `PutAuditEvents` per distribuire gli eventi al tuo canale. Il proprietario della risorsa ha accesso implicito alla risorsa se la sua policy IAM consente l'operazione `cloudtrail-data:PutAuditEvents`.

    Le informazioni richieste per la policy dipendono dal tipo di integrazione. Per un'integrazione direzionale, aggiunge CloudTrail automaticamente l' AWS account IDs del partner e richiede l'immissione dell'ID esterno univoco fornito dal partner. Per l'integrazione di una soluzione, è necessario specificare almeno un ID AWS account come principale e, facoltativamente, inserire un ID esterno per evitare confusioni.

    > **Note**
    >
    > Se non crei una policy delle risorse per il canale, solo il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale.

    a. Per un'integrazione diretta, inserisci l'ID esterno fornito dal partner. Il partner di integrazione fornisce un ID esterno univoco, come un ID account o una stringa generata casualmente, da utilizzare per evitare che l'integrazione incorra nel problema "confused deputy". Il partner ha la responsabilità di creare e fornire un ID esterno univoco.

Per consultare la documentazione del partner che descrive come trovare l'ID esterno, scegli How to find this? (Come trovarlo?).

> **Note**
>
> Se la policy delle risorse include un ID esterno, tutte le chiamate all'API `PutAuditEvents` devono includere tale ID. Tuttavia, se la policy non definisce un ID esterno, il partner può comunque chiamare l'API `PutAuditEvents` e specificare un parametro `externalId`.

b. Per un'integrazione con una soluzione, scegli Aggiungi AWS account per specificare ogni ID AWS account da aggiungere come principale nella politica.

16. Scegli Next (Successivo) per rivedere le scelte effettuate.
17. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
18. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.
19. Fornisci il nome della risorsa Amazon (ARN) del canale all'applicazione del partner. Le istruzioni per fornire l'ARN del canale all'applicazione del partner sono disponibili sul sito Web della documentazione dei partner. Per ulteriori informazioni, seleziona il link Learn more (Ulteriori informazioni) relativo al partner nella scheda Available sources (Origini disponibili) della pagina Integrations (Integrazioni) per aprire la pagina del partner in Marketplace AWS.

L'event data store inizia a importare gli eventi dei partner CloudTrail attraverso il canale di integrazione quando tu, il partner o le applicazioni partner chiamate l'`PutAuditEvents`API sul canale.

Aggiorna un data store di eventi con la console

In questa sezione viene descritto come aggiornare le impostazioni di un datastore di eventi utilizzando la AWS Management Console. Per informazioni su come aggiornare un event data store utilizzando il AWS CLI, vedereAggiornate un archivio dati di eventi con il AWS CLI.

Per aggiornare un datastore di eventi

1. Accedere a AWS Management Console e aprire la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegli il datastore di eventi da aggiornare. Questa operazione apre la pagina dei dettagli del datastore di eventi.
4. In Dettagli generali, scegli Modifica per modificare le impostazioni seguenti:
   - Nome dell'archivio di dati eventi: modifica il nome che identifica il tuo datastore di eventi.
   - Opzione di prezzo: per i datastore di eventi che utilizzano l'opzione Prezzo per la conservazione di sette anni, puoi scegliere di sostituire questa opzione con Prezzo per la conservazione estendibile di un anno. Consigliamo l'opzione Prezzo per la conservazione estendibile di un anno per i datastore di eventi che importano meno di 25 TB di dati di eventi al mese. Consigliamo l'opzione Prezzo per la conservazione estendibile di un anno anche se sei alla ricerca di un periodo di conservazione flessibile fino a 10 anni. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

     > **Note**
     >
     > Non puoi modificare l'opzione di prezzo per i datastore di eventi che utilizzano l'opzione Prezzo per la conservazione estendibile di un anno. Se desideri utilizzare l'opzione Prezzo per la conservazione di sette anni, interrompi l'importazione nel datastore di eventi corrente. Quindi crea un nuovo datastore di eventi con l'opzione Prezzo per la conservazione di sette anni.

   - Periodo di conservazione: modifica il periodo di conservazione per il datastore di eventi. Il periodo di conservazione determina la durata di conservazione dei dati degli eventi presenti nel datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

     > **Note**
     >
     > Se riduci il periodo di conservazione di un Event Data Store, CloudTrail rimuoverà tutti gli eventi con un periodo di conservazione `eventTime` precedente al nuovo. Ad esempio, se il periodo di conservazione precedente era di 365 giorni e lo riduci a 100

giorni, CloudTrail rimuoverà gli eventi con una data `eventTime` più vecchia di 100 giorni.

- Crittografia: per crittografare il datastore di eventi utilizzando la tua chiave KMS, scegli Usa la mia AWS KMS key. Per impostazione predefinita, tutti gli eventi in un archivio dati degli eventi sono crittografati da CloudTrail. L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia.

> **Note**
>
> Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

- Per includere solo gli eventi registrati nella Regione AWS corrente, scegli Includi solo la regione corrente nel mio datastore di eventi. Se non scegli questa opzione, il datastore di eventi include gli eventi provenienti da tutte le regioni.
- Per fare in modo che il tuo archivio dati degli eventi raccolga gli eventi da tutti gli account di un' AWS Organizations organizzazione, scegli Abilita per tutti gli account della mia organizzazione. Questa opzione è disponibile solo se hai effettuato l'accesso con l'account di gestione dell'organizzazione e il tipo di evento per il data store CloudTraildegli eventi è Eventi o Elementi di configurazione.

Al termine, scegli Salva le modifiche.

5. Nella federazione delle query di Lake, scegli Modifica per abilitare o disabilitare la federazione delle query di Lake. L'attivazione della federazione delle query di Lake consente di visualizzare i metadati per il data store degli eventi nel AWS Glue Data Catalog ed eseguire query SQL sui dati dell'evento utilizzando Amazon Athena. La disabilitazione della federazione delle query di Lake disabilita l'integrazione con AWS Glue AWS Lake Formation, e Amazon Athena. Dopo aver disabilitato la federazione delle query di Lake, non puoi più eseguire query sui dati in Athena. Nessun dato di CloudTrail Lake viene eliminato quando disabiliti la federazione e puoi continuare a eseguire query in Lake. CloudTrail

   Per abilitare la federazione, procedi come segue:

   a. Scegli Abilita .

b. Scegli se creare un nuovo ruolo IAM o se utilizzarne uno esistente. Quando crei un nuovo ruolo, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se utilizzi un ruolo esistente, assicurati che la policy del ruolo fornisca le autorizzazioni minime richieste.

c. Se crei un nuovo ruolo IAM, inserisci un nome per il ruolo.

d. Se scegli un ruolo IAM esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

Al termine, scegli Salva modifiche.

6. In Politica delle risorse, scegli Modifica per aggiungere o modificare la politica basata sulle risorse per l'archivio dati degli eventi.

   Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati

a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

7. Modifica eventuali impostazioni aggiuntive specifiche per il tipo di evento del tuo Event Data Store.

   Impostazioni per CloudTrail gli eventi

   - Per modificare gli eventi che l'archivio dati degli eventi registra, scegli Modifica negli CloudTrail eventi.
   - In Eventi di gestione, scegli Modifica per modificare le impostazioni degli eventi di gestione. Per ulteriori informazioni, consulta Aggiornamento delle impostazioni degli eventi di gestione per un archivio dati di eventi esistente.
   - In Eventi di dati, scegli Modifica per modificare le impostazioni degli eventi di dati. Puoi scegliere quali tipi di risorse vuoi registrare e scegliere il modello di selettore di log che desideri utilizzare. Per ulteriori informazioni, consulta Aggiornamento di un data store di eventi esistente per registrare gli eventi di dati utilizzando la console.
   - In Eventi di attività di rete, scegli Modifica per modificare le impostazioni relative agli eventi di attività di rete. Puoi scegliere il tipo di evento di attività di rete che desideri registrare e scegliere il modello di selettore di registro che desideri utilizzare. Per ulteriori informazioni, consulta Aggiornamento di un datastore di eventi esistente per registrare gli eventi di attività di rete.
   - In Arricchisci eventi, espandi la dimensione dell'evento, scegli Modifica per aggiungere o rimuovere tag di risorsa e chiavi di condizione globali IAM ed espandi la dimensione dell'evento.

     In Enrich events, aggiungi fino a 50 chiavi di tag di risorsa e 50 chiavi di condizione globali IAM per fornire metadati aggiuntivi sui tuoi eventi. Questo ti aiuta a classificare e raggruppare gli eventi correlati.

     Se aggiungi chiavi di tag di risorsa, CloudTrail includerà le chiavi di tag selezionate associate alle risorse coinvolte nella chiamata API. Gli eventi API relativi alle risorse eliminate non avranno tag di risorsa.

Se aggiungi chiavi di condizione globali IAM, CloudTrail includerà informazioni sulle chiavi di condizione selezionate che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione, sulla rete e sulla richiesta stessa.

Le informazioni sulle chiavi dei tag di risorsa e sulle chiavi di condizione globali IAM sono mostrate nel `eventContext` campo dell'evento. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.

> **Note**
>
> Se un evento contiene una risorsa che non appartiene alla regione dell'evento, non CloudTrail compilerà i tag per questa risorsa perché il recupero dei tag è limitato alla regione dell'evento.

Scegliete Espandi la dimensione dell'evento per espandere il payload dell'evento fino a 1 MB da 256 KB. Questa opzione viene abilitata automaticamente quando aggiungi chiavi di tag di risorsa o chiavi di condizione globale IAM per garantire che tutte le chiavi aggiunte siano incluse nell'evento.

L'espansione della dimensione dell'evento è utile per l'analisi e la risoluzione dei problemi degli eventi, poiché consente di visualizzare l'intero contenuto dei seguenti campi, purché il payload dell'evento sia inferiore a 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Per ulteriori informazioni su questi campi, consulta il contenuto dei CloudTrail record.

Al termine, scegli Salva le modifiche.

Impostazioni per Events from integration

In Integrazioni, scegli la tua integrazione. Quindi scegli Modifica per modificare le seguenti impostazioni:

- In Dettagli sull'integrazione, modifica il nome che identifica il canale dell'integrazione.
- In Luogo di consegna dell'evento, scegli la destinazione degli eventi.
- In Resource policy (Policy delle risorse), configura la policy delle risorse per il canale dell'integrazione.

Al termine, scegli Salva le modifiche.

Per ulteriori informazioni su queste impostazioni, consultare Crea un'integrazione con un CloudTrail partner tramite la console.

8. Per aggiungere, modificare o rimuovere i tag, scegli Modifica in Tag. Puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso al datastore di eventi. Al termine, scegli Salva le modifiche.

Interrompi e avvia l'acquisizione di eventi con la console

Per impostazione predefinita, i datastore di eventi sono configurati per importare eventi. È possibile impedire a un Event Data Store di importare eventi utilizzando la console, oppure. AWS CLI APIs

Le opzioni Avvia importazione e Interrompi ingestione sono disponibili solo negli archivi dati di eventi contenenti CloudTrail eventi (eventi di gestione, eventi di dati ed eventi di attività di rete) o elementi di configurazione. AWS Config

Quando si interrompe l'importazione su un datastore di eventi, lo stato datastore di eventi cambia in. `STOPPED_INGESTION` È comunque possibile eseguire query su qualsiasi evento già presente nel datastore di eventi. È inoltre possibile copiare gli eventi di trail nell'event data store (se contiene solo eventi). CloudTrail

Interruzione dell'importazione di eventi da parte di un datastore di eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.

3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Da Operazioni, scegli Interrompi importazione.
5. Quando viene chiesto di confermare l'operazione, seleziona Interrompi la registrazione. Il datastore di eventi smetterà di importare gli eventi live.
6. Per riprendere l'importazione, scegli Avvia importazione.

Per riavviare l'importazione degli eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Da Operazioni, scegli Avvia importazione.

Modificare la protezione dalla terminazione con la console

Per impostazione predefinita, i data store di eventi in AWS CloudTrail Lake sono configurati con la protezione dalla terminazione abilitata. La protezione della terminazione impedisce l'eliminazione accidentale dei datastore di eventi. Se desideri eliminare il datastore di eventi, devi disabilitare la protezione della terminazione. È possibile disabilitare la protezione dalla terminazione utilizzando le AWS Management Console operazioni AWS CLI, o API.

Per disattivare la protezione della terminazione

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Da Operazioni, scegli Modifica protezione della terminazione.
5. Scegli Disabilita.
6. Scegli Save (Salva). Ora puoi eliminare il data store degli eventi.

Per attivare la protezione della terminazione

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Da Operazioni, scegli Modifica protezione della terminazione.
5. Per attivare la protezione della terminazione, scegli Abilitata.
6. Scegli Save (Salva).

Eliminare un archivio dati di eventi con la console

In questa sezione viene descritto come eliminare un datastore di eventi utilizzando la console CloudTrail. Per informazioni su come eliminare un Event Data Store utilizzando il AWS CLI, vedereEliminare un archivio dati di eventi con AWS CLI.

> **Note**
>
> Non è possibile eliminare un datastore di eventi se è abilitata la protezione della terminazione o la federazione delle query di Lake. Per impostazione predefinita, CloudTrail abilita la protezione dalla terminazione per proteggere un Event Data Store dall'eliminazione accidentale.
>
> Per eliminare un datastore di eventi con un tipo di evento di Eventi dall'integrazione, devi prima eliminare il canale dell'integrazione. È possibile eliminare il canale dalla pagina dei dettagli dell'integrazione o utilizzando il comando aws cloudtrail delete-channel. Per ulteriori informazioni, consulta Eliminare un canale per eliminare un'integrazione con AWS CLI

Per eliminare un datastore di eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. In Operazioni, seleziona Elimina.
5. Digita il nome del datastore di eventi per confermare che desideri eliminarlo.

6. Scegliere Delete (Elimina).

Dopo l'eliminazione di un datastore di eventi, lo stato del datastore cambia in `PENDING_DELETION` e rimane tale per 7 giorni. È possibile ripristinare un datastore di eventi durante il periodo di 7 giorni. Mentre si trova nello stato `PENDING_DELETION`, il datastore di eventi non è disponibile per le query né consente di eseguire altre operazioni, tranne quelle di ripristino. Un datastore di eventi in attesa di eliminazione non acquisisce eventi e non comporta costi. I data store di eventi in attesa di eliminazione vengono conteggiati ai fini della quota di archivi dati di eventi che possono esistere in uno Regione AWS.

Ripristina un archivio dati di eventi con la console

Dopo aver eliminato un archivio dati di eventi in AWS CloudTrail Lake, il relativo stato cambia `PENDING_DELETION` e rimane tale per 7 giorni. Durante questo periodo, puoi ripristinare l'archivio dati degli eventi utilizzando l'operazione AWS Management Console AWS CLI, o l'RestoreEventDataStoreAPI.

In questa sezione viene descritto come ripristinare un datastore di eventi utilizzando la console. Per informazioni su come ripristinare un Event Data Store utilizzando il AWS CLI, vedereRipristina un archivio dati di eventi con AWS CLI.

Per ripristinare un datastore di eventi

1. Accedere a AWS Management Console e aprire la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Da Operazioni, scegli Ripristina.

Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI

Questa sezione descrive i AWS CLI comandi che puoi utilizzare per creare, aggiornare e gestire i tuoi archivi di dati di eventi CloudTrail Lake.

Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Comandi disponibili per gli archivi dati degli eventi

I comandi per la creazione e l'aggiornamento degli archivi di dati di eventi in CloudTrail Lake includono:

- `create-event-data-store`per creare un archivio dati di eventi.
- `get-event-data-store`per restituire informazioni sull'archivio dati degli eventi, inclusi i selettori di eventi avanzati configurati per l'archivio dati degli eventi.
- `update-event-data-store`per modificare la configurazione di un archivio dati di eventi esistente.
- `list-event-data-stores`per elencare gli archivi di dati degli eventi.
- `delete-event-data-store`per eliminare un archivio dati di eventi.
- `restore-event-data-store`per ripristinare un archivio dati di eventi in attesa di eliminazione.
- `start-import`per avviare un'importazione di eventi trail in un Event Data Store o riprovare un'importazione non riuscita.
- `get-import`per restituire informazioni su un'importazione specifica.
- `stop-import`per interrompere l'importazione di eventi trail in un data store di eventi.
- `list-imports`per restituire informazioni su tutte le importazioni o su un insieme selezionato di importazioni da `ImportStatus` o`Destination`.
- `list-import-failures`per elencare gli errori di importazione per l'importazione specificata.
- `stop-event-data-store-ingestion`per interrompere l'inserimento degli eventi in un archivio dati di eventi.
- `start-event-data-store-ingestion`per riavviare l'inserimento di eventi in un data store di eventi.
- `enable-federation`per abilitare la federazione su un data store di eventi per interrogare il data store di eventi in Amazon Athena.
- `disable-federation`per disabilitare la federazione su un data store di eventi. Dopo aver disabilitato la federazione, non puoi più eseguire query sui dati dell'Event Data Store in Amazon Athena. Puoi continuare a eseguire query in CloudTrail Lake.
- `put-insight-selectors`per aggiungere o modificare i selettori di eventi Insights per un data store di eventi esistente e abilitare o disabilitare gli eventi Insights.
- `get-insight-selectors`per restituire informazioni sui selettori di eventi Insights configurati per un archivio dati di eventi.

- `add-tags`per aggiungere uno o più tag (coppie chiave-valore) a un archivio dati di eventi esistente.
- `remove-tags`per rimuovere uno o più tag da un archivio dati di eventi.
- `list-tags`per restituire un elenco di tag associati a un archivio dati di eventi.
- `get-event-configuration`per restituire tutte le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM configurate per l'event data store. Il comando restituisce anche se l'event data store è configurato per raccogliere eventi relativi alle `Standard` dimensioni o agli eventi relativi `Large` alle dimensioni.
- `put-event-configuration`per espandere la dimensione dell'evento e aggiungere o rimuovere le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.
- `put-resource-policy`per allegare una policy basata sulle risorse a un archivio dati di eventi. Le policy basate sulle risorse consentono di controllare quali soggetti possono eseguire azioni sul data store degli eventi. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.
- `get-resource-policy`per allegare la policy basata sulle risorse a un archivio dati di eventi.
- `delete-resource-policy`per eliminare la politica basata sulle risorse allegata a un data store di eventi.

Per un elenco dei comandi disponibili per le query su CloudTrail Lake, consulta. Comandi disponibili per le query su CloudTrail Lake

Per un elenco dei comandi disponibili per le dashboard di CloudTrail Lake, consulta. Comandi disponibili per i dashboard

Per un elenco dei comandi disponibili per le integrazioni di CloudTrail Lake, consulta. Comandi disponibili per le integrazioni con CloudTrail Lake

Crea un data store di eventi con AWS CLI

Questa sezione descrive come utilizzare il `create-event-data-store`comando per creare un archivio dati di eventi e fornisce esempi di diversi tipi di archivi di dati di eventi che è possibile creare.

Quando crei un datastore di eventi, l'unico parametro richiesto è `--name`, che viene utilizzato per identificare tale datastore. È possibile configurare parametri opzionali aggiuntivi, tra cui:

- `--advanced-event-selectors`: specifica il tipo di eventi da includere nel datastore di eventi. Per impostazione predefinita, i datastore di eventi registrano tutti gli eventi di gestione. Per ulteriori informazioni sui selettori di eventi avanzati, consulta AdvancedEventSelectorl' CloudTrail API Reference.
- `--kms-key-id`- Speciifica l'ID della chiave KMS da utilizzare per crittografare gli eventi forniti da. CloudTrail Questo valore può essere un nome alias con il prefisso `alias/`, un ARN completo per un alias, un ARN completo per una chiave o un identificatore univoco globale.
- `--multi-region-enabled`- Crea un archivio dati di eventi multiregionale che registra gli eventi per tutti gli utenti del tuo account. Regioni AWS `--multi-region-enabled` è impostato per impostazione predefinita, anche se il parametro non viene aggiunto.
- `--organization-enabled`: consente a un datastore di eventi di raccogliere eventi per tutti gli account di un'organizzazione. Per impostazione predefinita, il datastore di eventi non è abilitato per tutti gli account di un'organizzazione.
- `--billing-mode`: determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi.

  Di seguito sono riportati i valori possibili:

  - `EXTENDABLE_RETENTION_PRICING`: questa modalità di fatturazione in genere è consigliata se importi meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 3.653 giorni (circa 10 anni). Il periodo di conservazione predefinito per questa modalità di fatturazione è 366 giorni.
  - `FIXED_RETENTION_PRICING`: questa modalità di fatturazione è consigliata se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 2.557 giorni (circa 7 anni). Il periodo di conservazione predefinito per questa modalità di fatturazione è 2.557 giorni.

  Il valore predefinito è `EXTENDABLE_RETENTION_PRICING`.
- `--retention-period`: il numero di giorni di conservazione degli eventi nel datastore di eventi. I valori validi sono numeri interi compresi tra 7 e 3.653 se la `--billing-mode` è `EXTENDABLE_RETENTION_PRICING` o tra 7 e 2.557 se la `--billing-mode` è impostata su `FIXED_RETENTION_PRICING`. Se non si specifica`--retention-period`, CloudTrail utilizza il periodo di conservazione predefinito per. `--billing-mode`
- `--start-ingestion`: il parametro `--start-ingestion` avvia l'importazione degli eventi nel datastore di eventi al momento della sua creazione. Questo parametro è impostato anche se non viene aggiunto.

Specifica `--no-start-ingestion` se desideri che il datastore di eventi non importi gli eventi live. Ad esempio, potresti voler impostare questo parametro se copi eventi nel datastore e prevedi di utilizzare i dati degli eventi solo per analizzare gli eventi passati. Il parametro `--no-start-ingestion` è valido solo se la `eventCategory` è `Management`, `Data` o `ConfigurationItem`.

Negli esempi seguenti viene illustrato come creare diversi tipi di datastore di eventi.

Esempi:

- Crea un archivio dati di eventi per gli eventi di dati S3 con il AWS CLI
- Crea un archivio dati di eventi per gli eventi di attività di rete KMS con AWS CLI
- Creare un archivio dati di eventi per gli elementi di AWS Config configurazione con AWS CLI
- Crea un archivio dati degli eventi organizzativi per gli eventi di gestione con il AWS CLI
- Crea archivi dati di eventi per gli eventi Insights con AWS CLI

Crea un archivio dati di eventi per gli eventi di dati S3 con il AWS CLI

Il seguente create-event-data-store comando di esempio AWS Command Line Interface (AWS CLI) crea un event data store denominato `my-event-data-store` che seleziona tutti gli eventi di dati di Amazon S3 e viene crittografato utilizzando una chiave KMS.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

Di seguito è riportata una risposta di esempio.

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Crea un archivio dati di eventi per gli eventi di attività di rete KMS con AWS CLI

L'esempio seguente mostra come creare un archivio dati di eventi per cui includere eventi di attività `VpceAccessDenied` di rete per AWS KMS. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi e il `eventSource` campo uguale a`kms.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
```

```
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Per ulteriori informazioni sugli eventi di attività di rete, vedereRegistrazione degli eventi delle attività di rete.

Creare un archivio dati di eventi per gli elementi di AWS Config configurazione con AWS CLI

Il AWS CLI create-event-data-store comando di esempio seguente crea un archivio dati di eventi denominato `config-items-eds` che seleziona gli elementi AWS Config di configurazione. Per raccogliere elementi di configurazione, specifica che il campo `eventCategory` è uguale a `ConfigurationItem` nei selettori di eventi avanzati.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
```

```
    }
]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

Crea un archivio dati degli eventi organizzativi per gli eventi di gestione con il AWS CLI

Il AWS CLI create-event-data-store comando di esempio seguente crea un archivio dati degli eventi organizzativi che raccoglie tutti gli eventi di gestione e imposta il `--billing-mode` parametro su`FIXED_RETENTION_PRICING`.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Crea archivi dati di eventi per gli eventi Insights con AWS CLI

Per registrare gli eventi di Insights in CloudTrail Lake, è necessario un data store di eventi di destinazione che raccolga gli eventi Insights e un data store di eventi di origine che abiliti Insights e registri gli eventi di gestione.

Questa procedura mostra come creare i datastore di eventi di destinazione e di origine e come abilitare gli eventi Insights.

1. Esegui il comando aws cloudtrail create-event-data-store per creare un datastore di eventi di destinazione che raccolga gli eventi di Insights. Il valore di `eventCategory` deve essere `Insight`. Sostituiscilo *`retention-period-days`* con il numero di giorni in cui desideri conservare gli eventi nel tuo archivio dati degli eventi. I valori validi sono numeri interi compresi tra 7 e 3.653 se la `--billing-mode` è `EXTENDABLE_RETENTION_PRICING` o tra 7 e 2.557 se la `--billing-mode` è impostata su `FIXED_RETENTION_PRICING`. Se non si specifica`--`

`retention-period`, CloudTrail utilizza il periodo di conservazione predefinito per`--billing-mode`.

Se hai effettuato l'accesso con l'account di gestione di un' AWS Organizations organizzazione, includi il `--organization-enabled` parametro se desideri concedere all'amministratore delegato l'accesso all'archivio dati degli eventi.

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
```

```
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Come valore per il parametro `--insights-destination` nel passaggio 3 utilizzerai l'ARN (o il suffisso ID dell'ARN) dalla risposta.

2. Esegui il comando aws cloudtrail create-event-data-store per creare un datastore di eventi di origine che registri gli eventi di gestione. Per impostazione predefinita, i datastore di eventi registrano tutti gli eventi di gestione. Non è necessario specificare i selettori di eventi avanzati se si desidera registrare tutti gli eventi di gestione. Sostituiscilo *`retention-period-days`* con il numero di giorni in cui desideri conservare gli eventi nel tuo archivio dati degli eventi. I valori validi sono numeri interi compresi tra 7 e 3.653 se la `--billing-mode` è `EXTENDABLE_RETENTION_PRICING` o tra 7 e 2.557 se la `--billing-mode` è impostata su `FIXED_RETENTION_PRICING`. Se non si specifica`--retention-period`, CloudTrail utilizza il periodo di conservazione predefinito per`--billing-mode`. Se stai creando un datastore di eventi dell'organizzazione, includi il parametro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
```

```
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Come valore per il parametro `--event-data-store` nel passaggio 3 utilizzerai l'ARN (o il suffisso ID dell'ARN) dalla risposta.

3. Esegui il comando put-insight-selectors per abilitare gli eventi Insights. I valori del selettore Insights possono essere`ApiCallRateInsight`, `ApiErrorRateInsight` o entrambi. Per il parametro `--event-data-store`, specifica l'ARN (o il suffisso ID dell'ARN) del datastore di eventi di origine che registra gli eventi di gestione e abiliterà Insights. Per il parametro `--insights-destination`, specifica l'ARN (o il suffisso ID dell'ARN) del datastore di eventi di destinazione che registrerà gli eventi di Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Il risultato seguente mostra il selettore di eventi Insights configurato per il datastore di eventi.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
```

```
            }
        ]
}
```

Dopo aver abilitato CloudTrail Insights per la prima volta su un archivio dati di eventi, CloudTrail potrebbero essere necessari fino a 7 giorni per iniziare a fornire gli eventi di Insights, a condizione che durante tale periodo venga rilevata un'attività insolita.

CloudTrail Insights analizza gli eventi di gestione che si verificano in una singola regione, non a livello globale. Un evento CloudTrail Insights viene generato nella stessa regione in cui vengono generati gli eventi di gestione di supporto.

Per un archivio dati di eventi organizzativi, CloudTrail analizza gli eventi di gestione dell'account di ciascun membro anziché analizzare l'aggregazione di tutti gli eventi di gestione dell'organizzazione.

Si applicano costi aggiuntivi per l'importazione di eventi Insights in Lake. CloudTrail Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

Importa gli eventi del trail in un data store di eventi con AWS CLI

Questa sezione mostra come creare e configurare un Event Data Store eseguendo il create-event-data-storecomando e quindi come importare gli eventi in tale Event Data Store utilizzando il start-importcomando. Per ulteriori informazioni sull'importazione di eventi trail, vedereCopia di eventi traccia in un archivio dati degli eventi.

Preparazione all'importazione degli eventi del percorso

Prima di importare gli eventi del percorso, effettua le seguenti operazioni preliminari.

- Assicurati di avere un ruolo con le autorizzazioni necessarie per importare gli eventi del percorso in un datastore di eventi.
- Determina il valore --billing-mode che desideri specificare per il datastore di eventi. La `--billing-mode` determina il costo dell'importazione e dell'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi.

  Quando importi gli eventi del trail su CloudTrail Lake, CloudTrail decomprime i log archiviati in formato gzip (compresso). Quindi CloudTrail copia gli eventi contenuti nei log nel tuo archivio dati

degli eventi. La dimensione dei dati non compressi potrebbe essere maggiore della dimensione di archiviazione effettiva di Amazon S3. Per avere una stima generale della dimensione dei dati non compressi, moltiplica la dimensione dei log nel bucket S3 per 10. Puoi utilizzare questa stima per scegliere il valore `--billing-mode` per il tuo caso d'uso.

- Determinate il valore che desiderate specificare per. `--retention-period` CloudTrail non copierà un evento se `eventTime` è più vecchio del periodo di conservazione specificato.

  Per determinare il periodo di conservazione corretto, calcola la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni per cui desideri conservare gli eventi nel datastore eventi, come dimostrato nell'equazione seguente:

  Periodo di conservazione = *`oldest-event-in-days`* + *`number-days-to-retain`*

  Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.
- Decidi se utilizzare il datastore di eventi per analizzare eventuali eventi futuri. Se non desideri importare eventi futuri, includi il parametro `--no-start-ingestion` durante la creazione del datastore di eventi. Per impostazione predefinita, i datastore di eventi iniziano a importare eventi quando vengono creati.

Per creare un datastore di eventi e importarvi gli eventi del percorso

1. Esegui il comando create-event-data-store per creare il nuovo datastore di eventi. In questo esempio, il `--retention-period` è impostato su `120` perché l'evento più vecchio copiato risale a 90 giorni fa e vogliamo conservare gli eventi per 30 giorni. Il parametro `--no-start-ingestion` è impostato perché non vogliamo importare eventi futuri. In questo esempio, `--billing-mode` non è stato impostato, perché utilizziamo il valore predefinito `EXTENDABLE_RETENTION_PRICING` dal momento che prevediamo di importare meno di 25 TB di dati di eventi.

   > **Note**
   >
   > Se stai creando il datastore di eventi per sostituire il percorso, ti consigliamo di configurarlo in modo che `--advanced-event-selectors` corrisponda ai selettori di eventi del percorso per assicurarti la stessa copertura degli eventi. Per impostazione predefinita, i datastore di eventi registrano tutti gli eventi di gestione.

```
aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
 120 --no-start-ingestion
```

Di seguito è riportata la risposta di esempio:

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

Lo `Status` iniziale è `CREATED` quindi eseguiremo il comando get-event-data-store per verificare che l'importazione sia interrotta.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

La risposta indica che ora lo `Status` è `STOPPED_INGESTION`, quindi al momento il datastore di eventi non importa gli eventi live.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. Usa il comando start-import per importare gli eventi del percorso nel datastore di eventi creato nella fase 1. Specifica l'ARN (o il suffisso ID dell'ARN) del datastore di eventi come valore per il parametro `--destinations`. Per `--start-event-time` specifica l'`eventTime` dell'evento più vecchio da copiare e per `--end-event-time` l'`eventTime` dell'evento più recente da copiare. Per `--import-source` specificare l'URI S3 per il bucket S3 contenente i log dei trail, il Regione AWS per il bucket S3 e l'ARN del ruolo utilizzato per importare gli eventi del trail.

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
```

```
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

Di seguito è riportata una risposta di esempio.

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Esegui il comando get-import per ottenere informazioni sull'importazione.

```
aws cloudtrail get-import --import-id import-id
```

Di seguito è riportata una risposta di esempio.

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
```

```
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

L'importazione termina con `ImportStatus` su `COMPLETED` se non si sono verificati errori o su `FAILED` se si sono verificati errori.

Se l'importazione ha registrato `FailedEntries`, puoi eseguire il comando list-import-failures per restituire un elenco di errori.

```
aws cloudtrail list-import-failures --import-id import-id
```

Per riprovare un'importazione che ha registrato errori, esegui il comando start-import solo con il parametro `--import-id`. Quando si riprova un'importazione, CloudTrail riprende l'importazione nella posizione in cui si è verificato l'errore.

```
aws cloudtrail start-import --import-id import-id
```

Aggiornate un archivio dati di eventi con il AWS CLI

Questa sezione fornisce esempi che mostrano come aggiornare le impostazioni di un event data store eseguendo il AWS CLI `update-event-data-store` comando.

Esempi:

- Aggiorna la modalità di fatturazione con AWS CLI
- Aggiornate la modalità di conservazione, attivate la protezione dalla terminazione e specificate a AWS KMS key con AWS CLI
- Disabilita la protezione dalla terminazione con AWS CLI

Aggiorna la modalità di fatturazione con AWS CLI

La `--billing-mode` per il datastore di eventi determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Se la `--billing-mode` di un datastore di eventi è impostata su `FIXED_RETENTION_PRICING`, puoi modificare il valore in `EXTENDABLE_RETENTION_PRICING`. In genere, `EXTENDABLE_RETENTION_PRICING` è consigliato se il datastore di eventi importa meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 3.653 giorni. Per informazioni sui prezzi, consulta Prezzo AWS CloudTrail e Gestione dei costi CloudTrail del lago.

> **Note**
>
> Non puoi modificare il valore della `--billing-mode` da `EXTENDABLE_RETENTION_PRICING` a `FIXED_RETENTION_PRICING`. Se la modalità di fatturazione del datastore di eventi è impostata su `EXTENDABLE_RETENTION_PRICING`, ma desideri utilizzare `FIXED_RETENTION_PRICING` al suo posto, puoi interrompere l'importazione nel datastore di eventi e crearne uno nuovo che utilizzi `FIXED_RETENTION_PRICING`.

Il AWS CLI update-event-data-store comando di esempio seguente modifica l'`--billing-mode`archivio dati degli eventi da `FIXED_RETENTION_PRICING` a`EXTENDABLE_RETENTION_PRICING`. Il valore del parametro `--event-data-store` richiesto è un ARN (o il suffisso ID dell'ARN) ed è obbligatorio; altri parametri sono facoltativi.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Aggiornate la modalità di conservazione, attivate la protezione dalla terminazione e specificate a AWS KMS key con AWS CLI

Il AWS CLI update-event-data-store comando di esempio seguente aggiorna un Event Data Store per modificarne il periodo di conservazione a 100 giorni e abilitare la protezione dalla terminazione. Il valore del parametro `--event-data-store` richiesto è un ARN (o il suffisso ID dell'ARN) ed è obbligatorio; altri parametri sono facoltativi. In questo esempio, viene aggiunto il parametro `--retention-period` per portare il periodo di conservazione a 100 giorni. Facoltativamente, puoi scegliere di abilitare AWS Key Management Service la crittografia e specificare an AWS KMS key aggiungendo `--kms-key-id` al comando e specificando una chiave KMS ARN come valore. `--termination-protection-enabled`viene aggiunto per abilitare la protezione dalla terminazione su un archivio dati di eventi in cui non era abilitata la protezione dalla terminazione.

Un archivio dati di eventi che registra gli eventi dall'esterno AWS non può essere aggiornato per registrare gli eventi. AWS Analogamente, un Event Data Store che registra gli AWS eventi non può essere aggiornato per registrare gli eventi dall'esterno. AWS

> **Note**
>
> Se si riduce il periodo di conservazione di un Event Data Store, CloudTrail rimuoverà tutti gli eventi con un periodo di conservazione `eventTime` precedente al nuovo. Ad esempio, se il periodo di conservazione precedente era di 365 giorni e lo riduci a 100 giorni, CloudTrail rimuoverà gli eventi con una data `eventTime` più vecchia di 100 giorni.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
```

```
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Disabilita la protezione dalla terminazione con AWS CLI

Per impostazione predefinita, la protezione della terminazione è abilitata in un datastore di eventi per proteggerlo dall'eliminazione accidentale. Non è possibile eliminare un datastore di eventi con la protezione della terminazione abilitata. Se desideri eliminare il datastore di eventi, devi prima disabilitare la protezione della terminazione.

Il AWS CLI update-event-data-store comando di esempio seguente disattiva la protezione dalla terminazione passando il parametro. `--no-termination-protection-enabled`

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
```

```
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Gestione degli archivi dati degli eventi con AWS CLI

Questa sezione descrive diversi altri comandi che è possibile eseguire per ottenere informazioni sui data store degli eventi, avviare e interrompere l'ingestione su un data store di eventi e abilitare e disabilitare la federazione su un data store di eventi.

Argomenti

- Ottieni un archivio dati di eventi con AWS CLI
- Elenca tutti gli archivi dati degli eventi in un account con AWS CLI
- Aggiungi le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM ed espandi le dimensioni dell'evento
- Ottieni la configurazione degli eventi per un data store di eventi
- Ottieni la politica basata sulle risorse per un data store di eventi con AWS CLI
- Associa una policy basata sulle risorse a un data store di eventi con AWS CLI
- Eliminare la politica basata sulle risorse allegata a un data store di eventi con AWS CLI
- Interrompi l'acquisizione su un data store di eventi con AWS CLI

- Avvia l'importazione su un data store di eventi con AWS CLI
- Abilitare la federazione in un datastore di eventi
- Disabilitare la federazione in un datastore di eventi
- Ripristina un archivio dati di eventi con AWS CLI

Ottieni un archivio dati di eventi con AWS CLI

Il AWS CLI get-event-data-store comando di esempio seguente restituisce informazioni sull'archivio dati degli eventi specificato dal `--event-data-store` parametro richiesto, che accetta un ARN o il suffisso ID dell'ARN.

```
aws cloudtrail get-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Di seguito è riportata una risposta di esempio. L'ora di creazione e dell'ultimo aggiornamento sono espressi nel formato `timestamp`.

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
```

```
                    "StartsWith": [
                        "arn:aws:s3:::amzn-s3-demo-bucket"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

Elenca tutti gli archivi dati degli eventi in un account con AWS CLI

Il AWS CLI list-event-data-stores comando di esempio seguente restituisce informazioni su tutti gli archivi di dati di eventi in un account, nella regione corrente. I parametri opzionali includono `--max-results`, che consente di specificare il numero massimo di risultati che desideri che il comando restituisca su una singola pagina. Se ci sono più risultati di quanto specificato dal valore `--max-results`, esegui nuovamente il comando aggiungendo il valore `NextToken` restituito per visualizzare la pagina dei risultati successiva.

```
aws cloudtrail list-event-data-stores
```

Di seguito è riportata una risposta di esempio.

```
{
```

```
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

Aggiungi le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM ed espandi le dimensioni dell'evento

Esegui il AWS CLI `put-event-configuration` comando per espandere la dimensione massima dell'evento e aggiungi fino a 50 chiavi di tag di risorsa e 50 chiavi di condizione globali IAM per fornire metadati aggiuntivi sui tuoi eventi.

Il comando `put-event-configuration` accetta gli argomenti seguenti:

- `--event-data-store`— Specificare l'ARN dell'archivio dati dell'evento o il suffisso ID dell'ARN. Questo parametro è obbligatorio.
- `--max-event-size`— Impostare per `Large` impostare la dimensione massima dell'evento su 1 MB. Per impostazione predefinita, il valore è`Standard`, che specifica una dimensione massima dell'evento di 256 KB.

> **Note**
>
> Per aggiungere le chiavi dei tag di risorsa o le chiavi delle condizioni globali IAM, è necessario impostare la dimensione dell'evento in modo `Large` da garantire che tutte le chiavi aggiunte siano incluse nell'evento.

- `--context-key-selectors`— Specificate il tipo di chiavi che desiderate includere negli eventi raccolti dal vostro event data store. Puoi includere chiavi di tag di risorsa e chiavi di condizione globali IAM. Le informazioni sui tag di risorsa aggiunti e sulle chiavi di condizione globali IAM sono mostrate nel `eventContext` campo dell'evento. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.
  - Imposta `Type` to `TagContext` per passare un array di un massimo di 50 chiavi di tag di risorsa. Se aggiungi tag di risorsa, CloudTrail gli eventi includeranno le chiavi dei tag selezionate associate alle risorse coinvolte nella chiamata API. Gli eventi API relativi alle risorse eliminate non avranno tag di risorsa.
  - Imposta `Type` to `RequestContext` per passare un array di un massimo di 50 chiavi di condizione globali IAM. Se aggiungi chiavi di condizione globali IAM, CloudTrail gli eventi includeranno informazioni sulle chiavi di condizione selezionate che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione, sulla rete e sulla richiesta stessa.

L'esempio seguente imposta la dimensione massima dell'evento `Large` e aggiunge due chiavi di tag di risorsa `myTagKey1` `emyTagKey2`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"TagContext", "Equals":["myTagKey1","myTagKey2"]}]'
```

L'esempio successivo imposta la dimensione massima dell'evento `Large` e aggiunge un IAM; global condition key (`aws:MultiFactorAuthAge`).

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"RequestContext", "Equals":
["aws:MultiFactorAuthAge"]}]'
```

L'ultimo esempio rimuove tutte le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM e imposta la dimensione massima dell'evento su`Standard`.

```
aws cloudtrail put-event-configuration \
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Standard \
--context-key-selectors
```

Ottieni la configurazione degli eventi per un data store di eventi

Esegui il AWS CLI `get-event-configuration` comando per restituire la configurazione degli eventi per un data store di eventi che raccoglie CloudTrail eventi. Questo comando restituisce la dimensione massima dell'evento ed elenca le chiavi dei tag di risorsa e le chiavi delle condizioni globali IAM (se presenti) incluse negli CloudTrail eventi.

```
aws cloudtrail get-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Ottieni la politica basata sulle risorse per un data store di eventi con AWS CLI

L'esempio seguente esegue il `get-resource-policy` comando su un archivio dati di eventi organizzativi.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

Poiché il comando è stato eseguito su un data store di eventi organizzativi, l'output mostra sia la politica basata sulle risorse fornita sia quella `DelegatedAdminResourcePolicy`generata per gli account amministratore delegati e. `333333333333` `111111111111`

```
{
  "ResourceArn": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207",
  "ResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "EdsPolicyA",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::666666666666:root"
      },
      "Action": [
        "cloudtrail:geteventdatastore",
        "cloudtrail:startquery",
```

```
        "cloudtrail:describequery",
        "cloudtrail:cancelquery",
        "cloudtrail:generatequery",
        "cloudtrail:generatequeryresultssummary"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  },
  "DelegatedAdminResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "Organization-EventDataStore-Auto-Generated-Delegated-Admin-Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["333333333333", "111111111111"]
      },
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CancelQuery",
        "cloudtrail:CreateEventDataStore",
        "cloudtrail:DeleteEventDataStore",
        "cloudtrail:DescribeQuery",
        "cloudtrail:DisableFederation",
        "cloudtrail:EnableFederation",
        "cloudtrail:GenerateQuery",
        "cloudtrail:GenerateQueryResultsSummary",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListQueries",
        "cloudtrail:ListTags",
        "cloudtrail:RemoveTags",
        "cloudtrail:RestoreEventDataStore",
        "cloudtrail:UpdateEventDataStore",
        "cloudtrail:StartEventDataStoreIngestion",
        "cloudtrail:StartQuery",
        "cloudtrail:StopEventDataStoreIngestion",
        "cloudtrail:UpdateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
```

```
    }]
  }
}
```

Associa una policy basata sulle risorse a un data store di eventi con AWS CLI

Per eseguire query su una dashboard durante un aggiornamento manuale o pianificato, è necessario allegare una policy basata sulle risorse a ogni archivio di dati di eventi associato a un widget sulla dashboard. Ciò consente a CloudTrail Lake di eseguire le query per tuo conto. Per ulteriori informazioni sulla politica basata sulle risorse, consulta. Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard

L'esempio seguente allega una policy basata sulle risorse a un archivio dati di eventi che consente di CloudTrail eseguire query su un dashboard quando il dashboard viene aggiornato. Sostituiscilo *account-id* con l'ID del tuo account, *eds-arn* con l'ARN dell'archivio dati degli eventi per il quale CloudTrail verranno eseguite le query e con *dashboard-arn* l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
 "eds-arn", "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

Di seguito è riportato un esempio di risposta.

JSON

```
{ "Version": "2012-10-17", "Statement": [{ "Sid": "EDSPolicy", "Effect":
    "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
event_data_store_ID",
    "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE",
    "AWS:SourceAccount": "123456789012" } } } ] }
```

Per ulteriori esempi di policy, vedereEsempi di policy basate su risorse per archivi di dati di eventi.

Eliminare la politica basata sulle risorse allegata a un data store di eventi con AWS CLI

Gli esempi seguenti eliminano la politica basata sulle risorse allegata a un archivio dati di eventi. Sostituisci *eds-arn* con l'ARN dell'archivio dati degli eventi.

```
aws cloudtrail delete-resource-policy --resource-arn eds-arn
```

Se ha esito positivo, questo comando non produrrà alcun output.

Interrompi l'acquisizione su un data store di eventi con AWS CLI

Il AWS CLI stop-event-data-store-ingestion comando di esempio seguente impedisce a un Event Data Store di importare eventi. Per interrompere l'importazione, il datastore di eventi `Status` deve essere `ENABLED` e `eventCategory` deve essere `Management`, `Data` o `ConfigurationItem`. Il datastore di eventi è specificato da `--event-data-store`, che accetta un ARN del datastore di eventi o il suffisso ID dell'ARN. Dopo l'esecuzione di stop-event-data-store-ingestion, lo stato del datastore di eventi diventerà `STOPPED_INGESTION`.

Il datastore di eventi conta per il tuo account un massimo di dieci datastore di eventi quando il suo stato è `STOPPED_INGESTION`.

```
aws cloudtrail stop-event-data-store-ingestion \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Se l'operazione riesce, non verrà generata alcuna risposta.

Avvia l'importazione su un data store di eventi con AWS CLI

Il AWS CLI start-event-data-store-ingestion comando di esempio seguente avvia l'inserimento di eventi in un data store di eventi. Per avviare l'importazione, il datastore di eventi `Status` deve essere `STOPPED_INGESTION` e `eventCategory` deve essere `Management`, `Data` o `ConfigurationItem`. Il datastore di eventi è specificato da `--event-data-store`, che accetta un ARN del datastore di eventi o il suffisso ID dell'ARN. Dopo l'esecuzione di start-event-data-store-ingestion, lo stato del datastore di eventi diventerà `ENABLED`.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Se l'operazione riesce, non verrà generata alcuna risposta.

Abilitare la federazione in un datastore di eventi

Per abilitare la federazione, esegui il comando aws cloudtrail enable-federation fornendo i parametri `--event-data-store` e `--role` richiesti. Per `--event-data-store`, fornisci l'ARN del datastore di eventi (o il suffisso ID dell'ARN). Per `--role`, fornisci l'ARN per il tuo ruolo di federazione. Il ruolo deve esistere nel tuo account e fornire le autorizzazioni minime richieste.

```
aws cloudtrail enable-federation \
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Questo esempio mostra come un amministratore delegato può abilitare la federazione in un datastore di eventi dell'organizzazione specificando l'ARN del datastore di eventi nell'account di gestione e l'ARN del ruolo di federazione nell'account amministratore delegato.

```
aws cloudtrail enable-federation \
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-
id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Disabilitare la federazione in un datastore di eventi

Per disabilitare la federazione nel datastore di eventi, esegui il comando aws cloudtrail disable-federation. L'archivio di dati degli eventi è specificato da `--event-data-store`, che accetta un ARN dell'archivio di dati degli eventi o il suffisso ID dell'ARN.

```
aws cloudtrail disable-federation \
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Se si tratta di un datastore di eventi dell'organizzazione, utilizza l'ID account dell'account di gestione.

Ripristina un archivio dati di eventi con AWS CLI

Il comando di esempio della AWS CLI restore-event-data-store seguente ripristina un archivio di dati degli eventi in attesa di eliminazione. L'archivio di dati degli eventi è specificato da `--event-data-`

`store`, che accetta un ARN dell'archivio di dati degli eventi o il suffisso ID dell'ARN. È possibile ripristinare un archivio di dati degli eventi eliminato solo entro il periodo di attesa di sette giorni dopo l'eliminazione.

```
aws cloudtrail restore-event-data-store \
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

La risposta include informazioni sull'archivio di dati degli eventi, inclusi il relativo ARN, i selettori di eventi avanzati e lo stato del ripristino.

Eliminare un archivio dati di eventi con AWS CLI

Questa sezione mostra come eliminare un archivio dati di eventi eseguendo il comando AWS CLI `delete-event-data-store`

Per eliminare un Event Data Store, specificare l'`--event-data-store`ARN dell'Event Data Store o il suffisso ID dell'ARN. Dopo l'esecuzione di delete-event-data-store, lo stato finale del datastore di eventi è `PENDING_DELETION` e il datastore di eventi viene eliminato automaticamente dopo un periodo di attesa di 7 giorni.

Dopo l'esecuzione di delete-event-data-store su un archivio di dati degli eventi, non è possibile eseguire list-queries, describe-query oppure get-query-results sulle query che utilizzano l'archivio di dati disabilitato. L'Event Data Store conta ai fini dell'account un massimo di dieci archivi dati di eventi in un periodo in Regione AWS cui è in attesa di eliminazione.

> **Note**
>
> Non è possibile eliminare un datastore di eventi se `--termination-protection-enabled` è impostato o se il suo `FederationStatus` è `ENABLED`.
> Per eliminare un event data store con un `eventCategory` of`ActivityAuditLog`, devi prima eliminare il canale dell'integrazione. È possibile eliminare il canale utilizzando il `aws cloudtrail delete-channel` comando. Per ulteriori informazioni, consulta Eliminare un canale per eliminare un'integrazione con AWS CLI.

```
aws cloudtrail delete-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Se l'operazione riesce, non verrà generata alcuna risposta.

Gestione dei cicli di vita dell'archivio di dati degli eventi

Di seguito sono riportate le fasi del ciclo di vita di un datastore di eventi:

- `CREATED`: uno stato a breve termine che indica che il datastore di eventi è stato creato.
- `ENABLED`: il datastore di eventi è attivo e importa gli eventi. Puoi eseguire query e copiare eventi di percorso nel datastore di eventi.
- `STARTING_INGESTION`: uno stato a breve termine che indica che il datastore di eventi inizierà a importare eventi live.
- `STOPPING_INGESTION`: uno stato a breve termine che indica che il datastore di eventi smetterà di importare eventi live.
- `STOPPED_INGESTION`: il datastore di eventi non importa gli eventi live. È comunque possibile eseguire query su qualsiasi evento già presente nel datastore di eventi e copiare gli eventi di percorso nel datastore.
- `PENDING_DELETION`: il datastore di eventi si trovava in uno stato `ENABLED` o `STOPPED_INGESTION` ed è stato eliminato, ma si trova nel periodo di attesa di 7 giorni prima dell'eliminazione definitiva. Non è possibile eseguire query sul datastore di eventi e non è possibile eseguire alcuna operazione tranne il ripristino.

È possibile eliminare un datastore di eventi solo se sia la federazione che la protezione della terminazione sono disabilitate. La protezione della terminazione impedisce l'eliminazione accidentale di un datastore di eventi. Per impostazione predefinita, negli archivi di dati degli eventi la protezione da cessazione è abilitata. La federazione consente di eseguire query sul datastore di eventi in Athena ed è disabilitata per impostazione predefinita.

Dopo l'eliminazione, un datastore di eventi rimane nello stato `PENDING_DELETION` per 7 giorni prima che venga eliminato definitivamente. È possibile ripristinare un datastore di eventi durante il periodo di 7 giorni. Quando è nello stato `PENDING_DELETION`, l'archivio di dati degli eventi non è disponibile per le query né consente di eseguire altre operazioni, tranne le operazioni di ripristino. Un datastore di eventi in attesa di eliminazione non acquisisce eventi e non comporta costi. Tuttavia, gli archivi dati di eventi in attesa di eliminazione vengono conteggiati ai fini della quota di archivi dati di eventi che possono esistere in uno Regione AWS di essi.

Azioni disponibili nei datastore di eventi

Per eliminare o ripristinare un Event Data Store, copiare gli eventi del trail, avviare o interrompere l'acquisizione di eventi o attivare o disattivare la protezione dalla terminazione di un Event Data Store, utilizza i comandi del menu Azioni della pagina dei dettagli dell'Event Data Store.

L'opzione Copia gli eventi del trail è disponibile solo nei data store di eventi che contengono eventi. CloudTrail Le opzioni Avvia importazione e Interrompi ingestione sono disponibili solo negli archivi di dati di eventi contenenti CloudTrail eventi (eventi di gestione e dati) o elementi di configurazione. AWS Config

Copia di eventi traccia in un archivio dati degli eventi

È possibile copiare gli eventi del percorso in un archivio dati di eventi CloudTrail Lake per creare un' point-in-timeistantanea degli eventi registrati nel percorso. La copia degli eventi traccia non interferisce con la capacità del percorso di registrare gli eventi e non modifica in alcun modo il percorso.

Puoi copiare gli eventi del trail in un data store di eventi esistente configurato per CloudTrail gli eventi oppure puoi creare un nuovo CloudTrail event data store e scegliere l'opzione Copia gli eventi del trail come parte della creazione del data store degli eventi. Per ulteriori informazioni sulla copia degli eventi di percorso in un datastore di eventi esistente, consulta Copia gli eventi del trail in un data store di eventi esistente con la console. Per ulteriori informazioni sulla creazione di un nuovo datastore di eventi, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

Se stai copiando gli eventi del trail in un datastore di eventi dell'organizzazione, dovrai utilizzare l'account di gestione dell'organizzazione. Non puoi copiare gli eventi del trail utilizzando l'account dell'amministratore delegato di un'organizzazione.

CloudTrail I data store di eventi Lake sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Quando copi gli eventi del trail in un CloudTrail Lake Event Data Store, ti vengono addebitati dei costi in base alla quantità di dati non compressi che l'Event Data Store acquisisce.

Quando copi gli eventi del trail su CloudTrail Lake, CloudTrail decomprime i log archiviati in formato gzip (compresso) e quindi copia gli eventi contenuti nei log nel tuo archivio dati degli eventi. La dimensione dei dati non compressi potrebbe essere maggiore della dimensione di archiviazione

effettiva di S3. Per avere una stima generale della dimensione dei dati non compressi, puoi moltiplicare la dimensione dei log nel bucket S3 per 10.

È possibile ridurre i costi specificando un intervallo di tempo più ristretto per gli eventi copiati. Se intendi utilizzare il datastore di eventi solo per le query sugli eventi copiati, puoi disattivare l'importazione degli eventi ed evitare così di incorrere in addebiti per eventi futuri. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

Scenari

La tabella seguente descrive alcuni scenari comuni per la copia degli eventi di percorso e come realizzare ogni scenario utilizzando la console.

Scenario	Come posso eseguire questa operazione nella console?
Analizza e interroga gli eventi storici del trail in Lake senza importare nuovi eventi CloudTrail	Crea un nuovo datastore di eventi e scegli l'opzione Copia gli eventi del percorso come parte della creazione del datastore di eventi. Durante la creazione del datastore di eventi, deselezio na Eventi di importazione (passaggio 15 della procedura) per assicurarti che il datastore di eventi contenga solo gli eventi storici del percorso e nessun evento futuro.
Sostituisci il percorso esistente con un archivio dati sugli eventi di CloudTrail Lake	Crea un datastore di eventi con gli stessi selettori di eventi del tuo percorso per assicurarti che il datastore di eventi abbia la stessa copertura del tuo percorso. Per evitare la duplicazione degli eventi tra il percorso di origine e il datastore di eventi di destinazione, scegli un intervallo di date per gli eventi copiati che sia precedente alla creazione del datastore di eventi. Dopo la creazione del datastore di eventi, potrai disattivare la registrazione per il percorso ed evitare così costi aggiuntivi.

Argomenti

- Considerazioni sulla copia di eventi di percorso
- Autorizzazioni necessarie per la copia di eventi traccia
- Copia gli eventi del trail in un data store di eventi esistente con la console

- Copia gli eventi del trail in un nuovo archivio dati di eventi con la console
- Visualizza i dettagli della copia dell'evento con la console CloudTrail

Considerazioni sulla copia di eventi di percorso

Quando copi eventi traccia, considera i fattori seguenti.

- Quando copi gli eventi del trail, CloudTrail utilizza l'operazione `GetObject`API S3 per recuperare gli eventi del trail nel bucket S3 di origine. Esistono alcune classi di archiviazione archiviata di S3, come i livelli recupero flessibile S3 Glacier, Deep Archive S3 Glacier, S3 Outposts e Deep Archive Piano intelligente Amazon S3 che non sono accessibili tramite l'utilizzo di `GetObject`. Per copiare gli eventi di percorso archiviati in queste classi di archiviazione archiviate, devi prima ripristinare una copia utilizzando l'operazione S3 `RestoreObject`. Per informazioni sul ripristino di oggetti archiviati, consulta Ripristino di oggetti archiviati nella Guida per l'utente di Amazon S3.
- Quando copi gli eventi di trail in un event data store, CloudTrail copia tutti gli eventi di trail indipendentemente dalla configurazione dei tipi di eventi dell'event data store di destinazione, dai selettori di eventi avanzati o. Regione AWS
- Prima di copiare gli eventi del percorso in un datastore di eventi esistente, assicurati che l'opzione di prezzo e il periodo di conservazione del datastore di eventi siano configurati correttamente per il tuo caso d'uso.
  - Opzione di prezzo: l'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi. Per ulteriori informazioni su opzioni di prezzo, consulta Prezzi AWS CloudTrail e Opzioni di prezzo del datastore di eventi.
  - Periodo di conservazione: il periodo di conservazione determina per quanto tempo i dati degli eventi vengono conservati nell'archivio dati degli eventi. CloudTrail copia solo gli eventi trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'Event Data Store (periodo di conservazione = *`oldest-event-in-days`* +*`number-days-to-retain`*). Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.
- Se stai copiando gli eventi di percorso in un datastore di eventi per analizzarli e non desideri importare eventi futuri, puoi interrompere l'importazione nel datastore. Durante la creazione del datastore di eventi, deseleziona l'opzione Eventi di importazione (passaggio 15 della procedura) per assicurarti che il datastore di eventi contenga solo gli eventi storici del percorso e nessun evento futuro.

- Prima di copiare gli eventi trail, disabilita tutte le liste di controllo degli accessi (ACLs) allegate al bucket S3 di origine e aggiorna la policy del bucket S3 per il data store degli eventi di destinazione. Per ulteriori informazioni sull'aggiornamento della policy del bucket S3, consulta Policy del bucket Amazon S3 per la copia di eventi traccia. Per ulteriori informazioni sulla disabilitazione ACLs, consulta Controllo della proprietà degli oggetti e disabilitazione del bucket. ACLs
- CloudTrail copia solo gli eventi trail dai file di registro compressi con Gzip che si trovano nel bucket S3 di origine. CloudTrail non copia gli eventi di trail da file di registro non compressi o file di registro compressi utilizzando un formato diverso da Gzip.
- Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, per gli eventi copiati scegli un intervallo di tempo precedente alla creazione dell'archivio dati degli eventi.
- Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel prefisso del bucket S3 e i `CloudTrail` prefissi all'interno del prefisso e non controlla i prefissi per `CloudTrail` altri servizi. AWS Se desideri copiare CloudTrail gli eventi contenuti in un altro prefisso, devi scegliere il prefisso quando copi gli eventi trail.
- Per copiare gli eventi del trail in un datastore di eventi dell'organizzazione, devi utilizzare l'account di gestione dell'organizzazione. Non puoi utilizzare l'account dell'amministratore delegato per copiare gli eventi di trail in un archivio dati di eventi di un'organizzazione.

Autorizzazioni necessarie per la copia di eventi traccia

Prima di copiare gli eventi trail, assicurati di disporre di tutte le autorizzazioni necessarie per il tuo ruolo IAM. Devi aggiornare le autorizzazioni del ruolo IAM solo se scegli un ruolo IAM esistente per la copia di eventi traccia. Se scegli di creare un nuovo ruolo IAM, CloudTrail fornisce tutte le autorizzazioni necessarie per il ruolo.

Se il bucket S3 di origine utilizza una chiave KMS per la crittografia dei dati, assicurati che la policy della chiave KMS CloudTrail consenta di decrittografare i dati nel bucket. Se il bucket S3 di origine utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail

Argomenti

- Autorizzazioni IAM per la copia di eventi traccia
- Policy del bucket Amazon S3 per la copia di eventi traccia
- Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine

Autorizzazioni IAM per la copia di eventi traccia

Quando copi eventi traccia, puoi creare un nuovo ruolo IAM o utilizzare un ruolo IAM esistente. Quando scegli un nuovo ruolo IAM, CloudTrail crea un ruolo IAM con le autorizzazioni richieste e non sono necessarie ulteriori azioni da parte tua.

Se scegli un ruolo esistente, assicurati che le policy del ruolo IAM consentano di copiare CloudTrail gli eventi del trail dal bucket S3 di origine. Questa sezione fornisce esempi delle policy di attendibilità e di autorizzazione necessarie al ruolo IAM.

L'esempio seguente fornisce la politica di autorizzazione, che consente di copiare gli eventi CloudTrail di trail dal bucket S3 di origine. Sostituisci*amzn-s3-demo-bucket*,*myAccountID*, *regionprefix*, e *eventDataStoreId* con i valori appropriati per la tua configurazione. *myAccountID*È l'ID dell' AWS account utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

Sostituisci *key-region* e *keyID* con i valori della chiave KMS utilizzata per crittografare il bucket S3 di origine. *keyAccountID* Se il bucket S3 di origine non utilizza una chiave KMS per la crittografia, puoi omettere l'istruzione `AWSCloudTrailImportKeyAccess`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
```

```
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

L'esempio seguente fornisce la policy di fiducia IAM, che consente di assumere un ruolo IAM CloudTrail per copiare gli eventi del trail dal bucket S3 di origine. Sostituisci *myAccountID* e *eventDataStoreArn* con i valori appropriati per la tua configurazione. *region* *myAccountID*È l' Account AWS ID utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
```

```
        }
      }
    }
  ]
}
```

Policy del bucket Amazon S3 per la copia di eventi traccia

Per impostazione predefinita, i bucket e gli oggetti Amazon S3 sono privati. Solo il proprietario della risorsa (l'account AWS che ha creato il bucket) può accedere al bucket e agli oggetti in esso contenuti. Il proprietario della risorsa può concedere le autorizzazioni di accesso ad altre risorse e ad altri utenti mediante una policy di accesso.

Prima di copiare gli eventi di trail, devi aggiornare la policy del bucket S3 per consentire CloudTrail di copiare gli eventi di trail dal bucket S3 di origine.

Puoi aggiungere la seguente dichiarazione alla policy del bucket S3 per concedere queste autorizzazioni. Sostituisci *roleArn* e *amzn-s3-demo-bucket* con i valori appropriati per la tua configurazione.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine

Se il bucket S3 di origine utilizza una chiave KMS per la crittografia dei dati, assicurati che la policy delle chiavi KMS fornisca le `kms:GenerateDataKey` autorizzazioni necessarie per copiare gli eventi del trail da un bucket S3 CloudTrail con la `kms:Decrypt` crittografia SSE-KMS abilitata. Se il bucket S3 di origine utilizza più chiavi KMS, è necessario aggiornare la policy di ogni chiave. L'aggiornamento della policy delle chiavi KMS consente di decrittografare i dati nel bucket S3 di origine, eseguire controlli di convalida CloudTrail per garantire che gli eventi siano conformi agli standard e copiare gli eventi nel Lake Event Data Store. CloudTrail CloudTrail

L'esempio seguente fornisce la politica delle chiavi KMS, che consente di CloudTrail decrittografare i dati nel bucket S3 di origine. Sostituisci*roleArn*,*amzn-s3-demo-bucket*, *myAccountIDregion*, e *eventDataStoreId* con i valori appropriati per la tua configurazione. *myAccountID*È l'ID dell' AWS account utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

Copia gli eventi del trail in un data store di eventi esistente con la console

Utilizza la procedura seguente per copiare eventi di percorso in un datastore di eventi esistente. Per ulteriori informazioni su come creare un nuovo datastore di eventi, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

> **Note**
>
> Prima di copiare gli eventi del percorso in un datastore di eventi esistente, assicurati che l'opzione di prezzo e il periodo di conservazione del datastore di eventi siano configurati correttamente per il tuo caso d'uso.
>
> - Opzione di prezzo: l'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi. Per ulteriori informazioni su opzioni di prezzo, consulta Prezzi AWS CloudTrail e Opzioni di prezzo del datastore di eventi.
> - Periodo di conservazione: il periodo di conservazione determina per quanto tempo i dati degli eventi vengono conservati nell'archivio dati degli eventi. CloudTrail copia solo gli eventi trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'Event Data Store (periodo di conservazione = *`oldest-event-in-days`* +*`number-days-to-retain`*). Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.

Per copiare eventi del percorso in un datastore di eventi

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Copy trail events (Copia eventi traccia).
4. Nella pagina Copy trail events (Copia eventi traccia), per Event source (Origine evento) scegliere il percorso da copiare. Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel `CloudTrail` prefisso del bucket S3 e i prefissi all'interno del prefisso e non controlla i `CloudTrail` prefissi per altri servizi. AWS Se desideri copiare gli CloudTrail eventi contenuti in un altro prefisso, scegli Inserisci URI S3, quindi scegli Browse S3 per cercare il

prefisso. Se il bucket S3 di origine per il percorso utilizza una chiave KMS per la crittografia dei dati, assicurati che la politica della chiave KMS consenta di decrittografare i dati. CloudTrail Se il tuo bucket S3 di origine utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail Per ulteriori informazioni sull'aggiornamento della policy delle chiavi KMS, consulta Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine.

La policy del bucket S3 deve consentire l' CloudTrail accesso alla copia degli eventi di trail dal bucket S3. Per ulteriori informazioni sull'aggiornamento della policy del bucket S3, consulta Policy del bucket Amazon S3 per la copia di eventi traccia.

5. Per Specificare un intervallo di tempo di eventi, scegli l'intervallo di tempo in cui copiare gli eventi. CloudTrail controlla il prefisso e il nome del file di registro per verificare che il nome contenga una data compresa tra la data di inizio e di fine scelte prima di tentare di copiare gli eventi del trail. Puoi scegliere un Intervallo relativo o un Intervallo assoluto. Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, scegliere un intervallo di tempo antecedente alla creazione dell'archivio dati degli eventi.

> **Note**
>
> CloudTrail copia solo gli eventi di trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Ad esempio, se il periodo di conservazione di un Event Data Store è di 90 giorni, non CloudTrail copierà alcun evento di trail con una data `eventTime` più vecchia di 90 giorni.

   - Se scegli Intervallo relativo, puoi scegliere di copiare gli eventi registrati negli ultimi 6 mesi, 1 anno, 2 anni, 7 anni o un intervallo personalizzato. CloudTrail copia gli eventi registrati nel periodo di tempo scelto.
   - Se scegli l'intervallo assoluto, puoi scegliere una data di inizio e di fine specifica. CloudTrail copia gli eventi che si sono verificati tra le date di inizio e di fine scelte.
6. Per Luogo di distribuzione, scegli l'archivio dati degli eventi di destinazione dall'elenco a discesa.
7. Per Autorizzazioni, scegli una delle opzioni seguenti del ruolo IAM. Se scegli un ruolo IAM esistente, accertati che la policy dei ruoli IAM fornisca le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiornamento delle autorizzazioni del ruolo IAM, consultare Autorizzazioni IAM per la copia di eventi traccia

- Scegli Creare un nuovo ruolo (consigliato) per creare un nuovo ruolo IAM. Per Inserisci il nome del ruolo IAM, inserisci un nome per il ruolo. CloudTrail crea automaticamente le autorizzazioni necessarie per questo nuovo ruolo.
- Scegli Usa un ruolo IAM personalizzato ARN per utilizzare un ruolo IAM personalizzato non elencato. Per Inserisci ARN ruolo IAM, inserisci l'ARN IAM.
- Scegli un ruolo IAM esistente dall'elenco a discesa.

8. Scegli Copia eventi.
9. Viene chiesto di confermare. Quando sei pronto a confermare, scegli Copia eventi traccia in Lake, quindi Copia eventi.
10. Nella pagina Dettagli copia, puoi visualizzare lo stato della copia ed esaminare eventuali errori. Quando la copia di un evento traccia viene completata, il relativo Stato copia viene impostato su Completato in assenza di errori o su Non riuscito se si sono verificati errori.

> **Note**
>
> I dettagli mostrati nella pagina dei dettagli della copia dell'evento non sono in tempo reale. I valori effettivi per dettagli come i prefissi copiati potrebbero essere superiori a quelli mostrati nella pagina. CloudTrail aggiorna i dettagli in modo incrementale nel corso della copia dell'evento.

11. Se Stato copia è Non riuscito, correggi eventuali errori mostrati in Errori di copia e scegli Riprova la copia. Quando si riprova una copia, la CloudTrail riprende nella posizione in cui si è verificato l'errore.

Per ulteriori informazioni sulla visualizzazione dei dettagli di una copia evento traccia, consulta Visualizza i dettagli della copia dell'evento con la console CloudTrail .

Copia gli eventi del trail in un nuovo archivio dati di eventi con la console

Questa procedura dettagliata mostra come copiare gli eventi del trail in un nuovo archivio dati di eventi CloudTrail Lake per l'analisi storica. Per ulteriori informazioni sulla copia di eventi di percorso, consulta Copia di eventi traccia in un archivio dati degli eventi.

Copia degli eventi di percorso in un nuovo datastore di eventi

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Scegliere Create event data store (Crea archivio di dati degli eventi).
4. Nella pagina Configura il data store degli eventi, in Dettagli generali, assegna un nome al tuo event data store, ad esempio`my-management-events-eds`. Come best practice, è consigliabile utilizzare un nome che identifichi in modo rapido lo scopo del datastore di eventi. Per informazioni sui requisiti di CloudTrail denominazione, consultaRequisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS.
5. Scegli l'opzione di prezzo che desideri utilizzare per il datastore di eventi. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché i periodi di conservazione predefiniti e quelli massimi per il tuo datastore di eventi. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

   Sono disponibili le seguenti opzioni:

   - Prezzo per la conservazione estendibile di un anno: consigliato in genere se prevedi di importare meno di 25 TB di dati di eventi al mese e desideri un periodo di conservazione flessibile fino a 10 anni. Per i primi 366 giorni (periodo di conservazione predefinito), l'archiviazione è inclusa senza alcun costo aggiuntivo nel prezzo di importazione. Dopo 366 giorni, la conservazione estesa è disponibile a prezzi pay-as-you-go convenienti. Questa è l'opzione predefinita.
     - Periodo di conservazione predefinito: 366 giorni
     - Periodo di conservazione massimo: 3.653 giorni
   - Prezzo per la conservazione di sette anni: consigliato se prevedi di importare più di 25 TB di dati di eventi al mese e hai bisogno di un periodo di conservazione fino a 7 anni. La conservazione è inclusa nel prezzo di importazione senza costi aggiuntivi.
     - Periodo di conservazione predefinito: 2.557 giorni
     - Periodo di conservazione massimo: 2.557 giorni
6. Specifica un periodo di conservazione per il datastore di eventi. I periodi di conservazione possono essere compresi tra 7 e 3.653 giorni (circa 10 anni) per l'opzione Prezzo per la conservazione estendibile di un anno o tra 7 e 2.557 giorni (circa sette anni) per l'opzione Prezzo per la conservazione di sette anni.

CloudTrail Lake determina se conservare un evento verificando se l'evento rientra nel periodo `eventTime` di conservazione specificato. Ad esempio, se si specifica un periodo di conservazione di 90 giorni, CloudTrail rimuoverà gli eventi quando `eventTime` sono più vecchi di 90 giorni.

> **Note**
>
> CloudTrail non copierà un evento se `eventTime` è più vecchio del periodo di conservazione specificato.
> Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'archivio dati degli eventi (periodo di conservazione = *`oldest-event-in-days`* +*`number-days-to-retain`*). Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.

7. (Facoltativo) In Crittografia, scegli se vuoi crittografare il datastore di eventi utilizzando la tua chiave KMS. Per impostazione predefinita, tutti gli eventi in un Event Data Store vengono crittografati CloudTrail utilizzando una chiave KMS che AWS possiede e gestisce per te.

   Per abilitare la crittografia utilizzando la tua chiave KMS, scegli Usa la mia AWS KMS key. Scegli Nuovo per AWS KMS key crearne uno personalizzato oppure scegli Esistente per utilizzare una chiave KMS esistente. In Inserisci alias KMS, specifica un alias nel formato. `alias/`*`MyAliasName`* L'utilizzo della propria chiave KMS richiede la modifica della politica delle chiavi KMS per consentire la crittografia e la decrittografia CloudTrail dei log. Per ulteriori informazioni, consulta. Configura le politiche AWS KMS chiave per CloudTrail CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

   L'utilizzo della propria chiave KMS comporta AWS KMS costi di crittografia e decrittografia. Dopo aver associato un datastore di eventi a una chiave KMS, la chiave KMS non potrà essere rimossa o modificata.

   > **Note**
   >
   > Per abilitare AWS Key Management Service la crittografia per un archivio dati di eventi organizzativi, è necessario utilizzare una chiave KMS esistente per l'account di gestione.

8. (Facoltativo) Se desideri eseguire una query sui dati degli eventi utilizzando Amazon Athena, scegli Abilita in Federazione delle query di Data Lake. La federazione ti consente di visualizzare i metadati associati al datastore di eventi nel Catalogo dati AWS Glue ed eseguire query SQL sui dati degli eventi in Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federare un datastore di eventi.

   Per abilitare la federazione delle query di Lake, scegli Abilita, quindi esegui queste operazioni:

   a. Scegli se creare un nuovo ruolo o utilizzare un ruolo IAM esistente. AWS Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se scegli un ruolo esistente, assicurati che la policy per il ruolo fornisca le autorizzazioni minime richieste.
   b. Se crei un nuovo ruolo, inserisci un nome per identificarlo.
   c. Se utilizzi un ruolo esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.

9. (Facoltativo) Scegli Abilita politica delle risorse per aggiungere una politica basata sulle risorse all'archivio dati degli eventi. Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi. Ad esempio, è possibile aggiungere una politica basata sulle risorse che consenta agli utenti root di altri account di interrogare questo archivio dati di eventi e visualizzare i risultati delle query. Per esempi di policy, consulta Esempi di policy basate su risorse per archivi di dati di eventi.

   Una politica basata sulle risorse include una o più istruzioni. Ogni dichiarazione della policy definisce i principali a cui è consentito o negato l'accesso all'Event Data Store e le azioni che i principali possono eseguire sulla risorsa Event Data Store.

   Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`

- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegato sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

10. (Facoltativo) In Tag, aggiungi uno o più tag personalizzati (coppie chiave-valore) al datastore di eventi. I tag possono aiutarti a identificare i tuoi archivi di dati sugli CloudTrail eventi. Ad esempio, è possibile allegare un tag con il nome **`stage`** e il valore **`prod`**. Puoi usare i tag per limitare l'accesso al datastore di eventi. Puoi utilizzare questi tag anche per tenere traccia dei costi di query e importazione per il datastore di eventi.

    Per informazioni su come controllare utilizzare i tag per monitorare i costi, consulta Creazione di tag di allocazione dei costi definiti dall'utente per i data store di CloudTrail eventi Lake. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un datastore di eventi in base ai tag, consulta Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per informazioni su come utilizzare i tag in AWS, consulta Tagging your AWS resources nella Tagging AWS Resources User Guide.

11. Scegli Next (Successivo) per configurare il datastore di eventi.
12. Nella pagina Scegli eventi, lascia le selezioni predefinite per Tipo di evento.
13. Per CloudTrail gli eventi, lasceremo selezionati gli eventi di gestione e sceglieremo Copia gli eventi del percorso. In questo esempio, non siamo preoccupati per i tipi di eventi perché utilizziamo il datastore di eventi solo per analizzare gli eventi passati e non stiamo importando eventi futuri.

    Se stai creando un datastore di eventi per sostituire un percorso esistente, scegli gli stessi selettori di eventi del percorso per assicurarti che il datastore di eventi abbia la stessa copertura dell'evento.

14. Scegli Abilita per tutti gli account della mia organizzazione se si tratta di un datastore di eventi dell'organizzazione. Questa opzione non sarà disponibile per la modifica, a meno che non ci siano già degli account in AWS Organizations.

> **Note**
>
> Se stai creando un datastore di eventi dell'organizzazione, devi accedere con l'account di gestione dell'organizzazione, poiché solo l'account di gestione può copiare gli eventi di percorso in un datastore di eventi dell'organizzazione.

15. Per Impostazioni aggiuntive, deselezioneremo Eventi di importazione, perché in questo esempio non vogliamo che il datastore di eventi importi eventi futuri poiché siamo interessati solo a interrogare gli eventi copiati. Per impostazione predefinita, un Event Data Store raccoglie eventi per tutti Regioni AWS e inizia a importarli al momento della creazione.
16. Per Eventi di gestione, lasceremo le impostazioni predefinite.
17. Nell'area Copia eventi di percorso, completa i seguenti passaggi.

    a. Scegliere il percorso che si vuole copiare. In questo esempio, sceglieremo un percorso denominato. *`management-events`*

       Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel `CloudTrail` prefisso del bucket S3 e i prefissi all'interno del prefisso e non controlla i `CloudTrail` prefissi per altri servizi. AWS Se desideri copiare gli CloudTrail eventi contenuti in un altro prefisso, scegli Inserisci URI S3, quindi scegli Browse S3 per cercare il prefisso. Se il bucket S3 di origine per il percorso utilizza una chiave KMS per la crittografia dei dati, assicurati che la politica della chiave KMS consenta di decrittografare i dati. CloudTrail Se il tuo bucket S3 di origine utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail Per ulteriori informazioni sull'aggiornamento della policy delle chiavi KMS, consulta Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine.

    b. Scegli un intervallo di tempo per copiare gli eventi. CloudTrail controlla il prefisso e il nome del file di registro per verificare che il nome contenga una data compresa tra la data di inizio e di fine scelte prima di tentare di copiare gli eventi del trail. Puoi scegliere un Intervallo relativo o un Intervallo assoluto. Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, scegliere un intervallo di tempo antecedente alla creazione dell'archivio dati degli eventi.

- Se scegli Intervallo relativo, puoi scegliere di copiare gli eventi registrati negli ultimi 6 mesi, 1 anno, 2 anni, 7 anni o un intervallo personalizzato. CloudTrail copia gli eventi registrati nel periodo di tempo scelto.
- Se scegli l'intervallo assoluto, puoi scegliere una data di inizio e di fine specifica. CloudTrail copia gli eventi che si sono verificati tra le date di inizio e di fine scelte.

In questo esempio, sceglieremo Absolute range e selezioneremo l'intero mese di maggio.

c. Per Autorizzazioni, scegli una delle opzioni seguenti del ruolo IAM. Se scegli un ruolo IAM esistente, accertati che la policy dei ruoli IAM fornisca le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiornamento delle autorizzazioni del ruolo IAM, consultare Autorizzazioni IAM per la copia di eventi traccia

- Scegli Creare un nuovo ruolo (consigliato) per creare un nuovo ruolo IAM. Per Inserisci il nome del ruolo IAM, inserisci un nome per il ruolo. CloudTrail crea automaticamente le autorizzazioni necessarie per questo nuovo ruolo.
- Scegli Usa un ruolo IAM personalizzato ARN per utilizzare un ruolo IAM personalizzato non elencato. Per Inserisci ARN ruolo IAM, inserisci l'ARN IAM.
- Scegli un ruolo IAM esistente dall'elenco a discesa.

In questo esempio, sceglieremo Crea un nuovo ruolo (consigliato) e gli assegneremo il nome **`copy-trail-events`**.

18. Scegli Next (Successivo) per rivedere le scelte effettuate.
19. Nella pagina Review and create (Rivedi e crea), esaminare le opzioni selezionate. Scegliere Edit (Modifica) per apportare modifiche a una sezione. Quando si è pronti a creare l'archivio di dati degli eventi, scegliere Create event data store (Crea archivio di dati degli eventi).
20. Il nuovo datastore di eventi sarà presente nella tabella Datastore di eventi sulla pagina Datastore di eventi.

21. Scegli il nome del datastore di eventi per visualizzarne la pagina dei dettagli. La pagina dei dettagli mostra i dettagli del tuo datastore di eventi e lo stato della copia. Lo stato della copia dell'evento viene visualizzato nell'area Stato della copia dell'evento.

Quando la copia di un evento traccia viene completata, il relativo Stato copia viene impostato su Completato in assenza di errori o su Non riuscito se si sono verificati errori.

22. Per visualizzare maggiori dettagli sulla copia, scegliete il nome della copia nella colonna Posizione S3 del log di eventi oppure scegli l'opzione Visualizza dettagli dal menu Operazioni. Per ulteriori informazioni sulla visualizzazione dei dettagli di una copia evento traccia, consulta Visualizza i dettagli della copia dell'evento con la console CloudTrail .

23. L'area Errori di copia mostra tutti gli errori che si sono verificati durante la copia degli eventi di percorso. Se Stato copia è Non riuscito, correggi eventuali errori mostrati in Errori di copia e scegli Riprova la copia. Quando riprovate una copia, la CloudTrail riprende nella posizione in cui si è verificato l'errore.

Visualizza i dettagli della copia dell'evento con la console CloudTrail

Dopo l'avvio della copia di un evento di percorso, è possibile visualizzare i dettagli della copia dell'evento, tra cui lo stato della copia e le informazioni su eventuali errori di copia.

> **Note**
>
> I dettagli mostrati nella pagina dei dettagli della copia dell'evento non sono in tempo reale. I valori effettivi per dettagli come i prefissi copiati potrebbero essere superiori a quelli mostrati nella pagina. CloudTrail aggiorna i dettagli in modo incrementale nel corso della copia dell'evento.

Per accedere alla pagina dei dettagli della copia dell'evento

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione sulla sinistra, seleziona Datastore di eventi in Lake.
3. Scegliere l'evento dall'archivio di dati degli eventi.
4. Scegliere la copia dell'evento nella sezione Event copy status (Stato della copia dell'evento).

Dettagli della copia

Da Copy details (Dettagli copia), è possibile visualizzare i dettagli seguenti sulla copia dell'evento di percorso.

- Event log S3 location (Posizione di S3 del registro degli eventi): la posizione del bucket S3 di origine contenente i file di log degli eventi traccia.
- Copy ID (ID copia): l'ID della copia.
- Prefixes copied (Prefissi copiati): rappresenta il numero di prefissi S3 copiati. Durante la copia di un evento di trail, CloudTrail copia gli eventi nei file di log del trail memorizzati nei prefissi.
- Copy status (Stato copia): lo stato della copia.
  - Initialization (nizializzazione): lo stato iniziale visualizzato all'avvio della copia dell'evento di percorso.
  - In progress (In corso): indica che la copia dell'evento di percorso è in corso.

    > **Note**
    >
    > Non è possibile copiare eventi traccia se un'altra copia di eventi traccia è In progress (In corso). Per interrompere la copia di un evento di percorso, scegliere Stop copy (Interrompi copia).

  - Stopped (Interrotto): indica che si è verificata un'azione Stop copy (Interrompi copia). Per riprovare la copia di un evento traccia, scegli Riprova copia.
  - Failed (Non riuscita): la copia è stata completata, ma alcuni eventi traccia non sono stati copiati. Esamina i messaggi di errore in Copy failures (Errori di copia). Per riprovare la copia di un evento traccia, scegli Riprova copia. Quando si riprova una copia, la CloudTrail riprende nella posizione in cui si è verificato l'errore.
  - Completed (Completata): la copia è stata completata senza errori. È possibile eseguire query degli eventi traccia copiati nelil datastore di eventi.
- Created time (Ora di creazione): indica quando è iniziata la copia dell'evento di percorso.
- Finish time (Ora di fine): indica quando è stata completata o interrotta la copia dell'evento di percorso.

Errori di copia

Da Copy failured (Errori di copia) è possibile esaminare la posizione dell'errore, il messaggio di errore e il tipo di errore per ogni errore di copia. Le cause più comuni di errore includono se un prefisso S3 conteneva un file non compresso o conteneva un file fornito da un servizio diverso da. CloudTrail Un'altra possibile causa di errore è correlata a problemi di accesso. Ad esempio, se il bucket S3 dell'Event Data Store non concedesse CloudTrail l'accesso all'importazione degli eventi, si verificherebbe un errore. `AccessDenied`

Per ogni errore di copia, consultare le informazioni seguenti sull'errore.

- Error location (Posizione dell'errore): indica la posizione nel bucket S3 in cui si è verificato l'errore. Se si è verificato un errore perché il bucket S3 di origine conteneva un file non compresso, Error location (Posizione dell'errore) include il prefisso in cui si trova tale file.
- Error message (Messaggio di errore): fornisce una spiegazione del motivo dell'errore.
- Error type (Tipo di errore): fornisce il tipo di errore. Ad esempio, un Error type (Tipo di errore) di `AccessDenied` indica che l'errore si è verificato a causa di un problema di autorizzazioni. Per ulteriori informazioni sulle autorizzazioni necessarie per la copia di eventi traccia, consultare Autorizzazioni necessarie per la copia di eventi traccia.

Dopo aver risolto eventuali errori, scegliere Retry copy (Riprova copia). Quando riprovi una copia, CloudTrail riprende la copia nella posizione in cui si è verificato l'errore.

Federare un datastore di eventi

La federazione di un data store di eventi consente di visualizzare i metadati associati al data store degli eventi nel AWS Glue Data Catalog, di registrare il Data Catalog e di eseguire query SQL sui dati degli eventi utilizzando Amazon Athena. AWS Lake Formation I metadati delle tabelle archiviati nel AWS Glue Data Catalog consentono al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare.

Puoi abilitare la federazione utilizzando la CloudTrail console o il funzionamento AWS CLI dell'EnableFederationAPI. Quando abiliti la federazione delle query di Lake, CloudTrail crea un database gestito denominato `aws:cloudtrail` (se il database non esiste già) e una tabella federata gestita nel AWS Glue Data Catalog. L'ID del data store degli eventi viene utilizzato per il nome della tabella. CloudTrail registra il ruolo di federazione AWS Lake Formationin cui ARN e event data store, il servizio responsabile di consentire il controllo granulare degli accessi alle risorse federate nel Data Catalog. AWS Glue

Per abilitare la federazione delle query di Lake, devi creare un nuovo ruolo IAM o scegliere un ruolo esistente. Lake Formation utilizza questo ruolo per gestire le autorizzazioni per il datastore di eventi federato. Quando crei un nuovo ruolo utilizzando la CloudTrail console, crea CloudTrail automaticamente le autorizzazioni richieste per il ruolo. Se scegli un ruolo esistente, assicurati che fornisca le autorizzazioni minime richieste.

È possibile disabilitare la federazione utilizzando la CloudTrail console o AWS CLI l'operazione DisableFederationAPI. Quando disabiliti la federazione, CloudTrail disabilita l'integrazione con AWS Glue e Amazon Athena. AWS Lake Formation Dopo aver disabilitato la federazione delle query di Lake, non puoi più eseguire query sui dati degli eventi in Athena. Nessun dato di CloudTrail Lake viene eliminato quando disabiliti la federazione e puoi continuare a eseguire query in Lake. CloudTrail

Non sono CloudTrail previsti costi per la federazione di un archivio dati di eventi CloudTrail Lake. L'esecuzione delle query in Amazon Athena è soggetta a costi. Per ulteriori informazioni sui prezzi di Athena, consulta Prezzi di Amazon Athena.

Analizza i registri delle attività con AWS CloudTrail Lake e Amazon Athena

Argomenti

- Considerazioni
- Autorizzazioni necessarie per la federazione
- Abilitare la federazione delle query di Lake
- Disabilitare la federazione delle query di Lake
- Gestione delle risorse della federazione dei CloudTrail laghi con AWS Lake Formation

Considerazioni

Considera i seguenti fattori durante la federazione di un datastore di eventi:

- Non sono CloudTrail previsti costi per la federazione di un archivio dati di eventi CloudTrail Lake. L'esecuzione delle query in Amazon Athena è soggetta a costi. Per ulteriori informazioni sui prezzi di Athena, consulta Prezzi di Amazon Athena.
- Lake Formation viene utilizzato per gestire le autorizzazioni per le risorse federate. Se elimini il ruolo federativo o revochi le autorizzazioni per le risorse da Lake Formation oppure AWS Glue, non puoi eseguire query da Athena. Per ulteriori informazioni sull'utilizzo di Lake Formation, consulta Gestione delle risorse della federazione dei CloudTrail laghi con AWS Lake Formation.

- Chiunque utilizzi Amazon Athena per eseguire query sui dati registrati con Lake Formation deve disporre di una policy di autorizzazione IAM che consente l'operazione `lakeformation:GetDataAccess`. La politica AWS gestita: consente questa azione. AmazonAthenaFullAccess Se utilizzi policy inline, assicurati di aggiornare le policy di autorizzazione per consentire questa operazione. Per ulteriori informazioni, consulta Gestione delle autorizzazioni utente Lake Formation e Athena.
- Per creare viste su tabelle federate in Athena, è necessario un database di destinazione diverso da `aws:cloudtrail`, Questo perché il `aws:cloudtrail` database è gestito da CloudTrail.
- Per creare un set di dati in Amazon QuickSight, devi scegliere l'opzione Usa SQL personalizzato. Per ulteriori informazioni, consulta Creazione di un set di dati utilizzando dati di Amazon Athena.
- Se la federazione è abilitata, non è possibile eliminare un datastore di eventi. Per eliminare un datastore di eventi federato, devi prima disabilitare la federazione e la protezione della terminazione (se abilitata).
- Le seguenti considerazioni si applicano ai datastore di eventi dell'organizzazione:
  - Solo un singolo account amministratore delegato o l'account di gestione può abilitare la federazione in un datastore di eventi dell'organizzazione. Altri account amministratore delegato possono comunque eseguire query e condividere informazioni utilizzando la funzionalità di condivisione dei dati di Lake Formation.
  - Qualsiasi account amministratore delegato o l'account di gestione dell'organizzazione può disabilitare la federazione.

Autorizzazioni necessarie per la federazione

Prima di federare un datastore di eventi, accertati di disporre di tutte le autorizzazioni necessarie per il ruolo di federazione e per abilitare e disabilitare la federazione. Per abilitare la federazione, devi aggiornare le autorizzazioni del ruolo di federazione solo se scegli un ruolo IAM esistente. Se scegli di creare un nuovo ruolo IAM utilizzando la CloudTrail console, CloudTrail fornisce tutte le autorizzazioni necessarie per il ruolo.

Argomenti

- Autorizzazioni IAM per la federazione di un datastore di eventi
- Autorizzazioni necessarie per l'abilitazione della federazione
- Autorizzazioni necessarie per la disabilitazione della federazione

Autorizzazioni IAM per la federazione di un datastore di eventi

Quando abiliti la federazione, puoi creare un nuovo ruolo IAM o utilizzare un ruolo IAM esistente. Quando scegli un nuovo ruolo IAM, CloudTrail crea un ruolo IAM con le autorizzazioni richieste e non sono necessarie ulteriori azioni da parte tua.

Se scegli un ruolo esistente, accertati che le policy dei ruoli IAM forniscano le autorizzazioni necessarie per abilitare la federazione. Questa sezione fornisce esempi delle policy di attendibilità e di autorizzazione necessarie al ruolo IAM.

L'esempio seguente fornisce la policy delle autorizzazioni per il ruolo di federazione. Per la prima istruzione, fornisci l'ARN completo del datastore di eventi per la `Resource`.

La seconda istruzione di questa policy consente a Lake Formation di decrittare i dati di un datastore di eventi crittografato con una chiave KMS. Sostituisci *`key-region`* e *`key-id`* con i valori della tua chiave KMS. *`account-id`* Se il datastore di eventi non utilizza una chiave KMS per la crittografia, puoi omettere questa istruzione.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "LakeFederationKMSDecryptAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id"
        }
    ]
}
```

L'esempio seguente fornisce la policy di attendibilità IAM che consente a AWS Lake Formation di assumere un ruolo IAM per la gestione delle autorizzazioni per il datastore di eventi federato.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Autorizzazioni necessarie per l'abilitazione della federazione

La policy di esempio seguente fornisce le autorizzazioni minime richieste per abilitare la federazione in un datastore di eventi. Questa policy consente di CloudTrail abilitare la federazione nell'archivio dati degli eventi, di AWS Glue creare le risorse federate nel AWS Glue Data Catalog e di AWS Lake Formation gestire la registrazione delle risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailEnableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "FederationRoleAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/federation-role-name"
        },
        {
            "Sid": "GlueResourceCreation",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-
id",
                "arn:aws:glue:us-east-1:111111111111:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "LakeFormationRegistration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource":
 "arn:aws:lakeformation:region:111111111111:catalog:111111111111"
        }
    ]
}
```

Autorizzazioni necessarie per la disabilitazione della federazione

La policy di esempio seguente fornisce le risorse minime richieste per disabilitare la federazione in un datastore di eventi. Questa politica consente di CloudTrail disabilitare la federazione sul data store degli eventi, di AWS Glue eliminare la tabella federata gestita nel AWS Glue Data Catalog e di Lake Formation di annullare la registrazione della risorsa federata.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailDisableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "GlueTableDeletion",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "LakeFormationDeregistration",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:us-
east-1:111111111111:catalog:111111111111"
        }
    ]
}
```

Abilitare la federazione delle query di Lake

Puoi abilitare la federazione delle query di Lake utilizzando la CloudTrail console o AWS CLI l'operazione EnableFederationAPI. Quando abiliti la federazione delle query di Lake, CloudTrail crea un database gestito denominato `aws:cloudtrail` (se il database non esiste già) e una tabella federata gestita nel AWS Glue Data Catalog. L'ID del data store degli eventi viene utilizzato per il nome della tabella. CloudTrail registra il ruolo di federazione AWS Lake Formationin cui ARN e

event data store, il servizio responsabile di consentire il controllo granulare degli accessi alle risorse federate nel Data Catalog. AWS Glue

Questa sezione descrive come abilitare la federazione utilizzando la console e. CloudTrail AWS CLI

CloudTrail console

La procedura seguente mostra come abilitare la federazione delle query di Lake in un datastore di eventi esistente.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegli il datastore di eventi da aggiornare. In questo modo si apre la pagina dei dettagli del datastore di eventi.
4. In Federazione delle query di Lake, scegli Modifica, quindi Abilita.
5. Scegli se creare un nuovo ruolo IAM o se utilizzarne uno esistente. Quando crei un nuovo ruolo, crea CloudTrail automaticamente un ruolo con le autorizzazioni richieste. Se utilizzi un ruolo esistente, assicurati che la policy del ruolo fornisca le autorizzazioni minime richieste.
6. Se crei un nuovo ruolo IAM, inserisci un nome per il ruolo.
7. Se scegli un ruolo IAM esistente, scegli il ruolo che desideri utilizzare. Il ruolo deve esistere nell'account.
8. Scegli Save changes (Salva modifiche). Lo stato della federazione cambia in `Enabled`.

AWS CLI

Per abilitare la federazione, esegui il comando aws cloudtrail enable-federation fornendo i parametri --event-data-store e --role richiesti. Per --event-data-store, fornisci l'ARN del datastore di eventi (o il suffisso ID dell'ARN). Per --role, fornisci l'ARN per il tuo ruolo di federazione. Il ruolo deve esistere nel tuo account e fornire le autorizzazioni minime richieste.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Questo esempio mostra come un amministratore delegato può abilitare la federazione in un datastore di eventi dell'organizzazione specificando l'ARN del datastore di eventi nell'account di gestione e l'ARN del ruolo di federazione nell'account amministratore delegato.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Disabilitare la federazione delle query di Lake

È possibile disabilitare la federazione utilizzando la CloudTrail AWS CLI console o l'operazione DisableFederationAPI. Quando disabiliti la federazione, CloudTrail disabilita l'integrazione con AWS Glue e Amazon Athena. AWS Lake Formation Dopo aver disabilitato la federazione delle query di Lake, non puoi più eseguire query sui dati degli eventi in Athena. Nessun dato di CloudTrail Lake viene eliminato quando disabiliti la federazione e puoi continuare a eseguire query in Lake. CloudTrail

Questa sezione descrive come disabilitare la federazione utilizzando la CloudTrail console e AWS CLI.

CloudTrail console

La procedura seguente mostra come disabilitare la federazione delle query di Lake in un datastore di eventi esistente.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegli il datastore di eventi da aggiornare. In questo modo si apre la pagina dei dettagli del datastore di eventi.
4. In Federazione delle query di Lake, scegli Modifica, quindi Disabilita.
5. Scegli Save changes (Salva modifiche). Lo stato della federazione cambia in `Disabled`.

AWS CLI

Per disabilitare la federazione nel datastore di eventi, esegui il comando aws cloudtrail disable-federation. L'archivio di dati degli eventi è specificato da `--event-data-store`, che accetta un ARN dell'archivio di dati degli eventi o il suffisso ID dell'ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Se si tratta di un datastore di eventi dell'organizzazione, utilizza l'ID account dell'account di gestione.

Gestione delle risorse della federazione dei CloudTrail laghi con AWS Lake Formation

Quando si federa un Event Data Store, CloudTrail registra il ruolo di federazione ARN e Event Data Store AWS Lake Formation, il servizio responsabile di consentire il controllo granulare degli accessi alle risorse federate nel Data Catalog. AWS Glue Questa sezione descrive come utilizzare Lake Formation per gestire le risorse della CloudTrail Lake Federation.

Quando abiliti la federazione, CloudTrail crea le seguenti risorse nel AWS Glue Data Catalog.

- Database gestito: CloudTrail crea 1 database con il nome `aws:cloudtrail` per account. CloudTrail gestisce il database. Non è possibile eliminare o modificare il database in AWS Glue.
- Tabella federata gestita: CloudTrail crea 1 tabella per ogni data store federato di eventi e utilizza l'ID del data store degli eventi per il nome della tabella. CloudTrail gestisce le tabelle. Non è possibile eliminare o modificare le tabelle in AWS Glue. Per eliminare una tabella, è necessario disabilitare la federazione nel datastore di eventi.

Controllo dell'accesso alle risorse federate

È possibile utilizzare uno dei due metodi di autorizzazione per controllare l'accesso al database e alle tabelle gestiti.

- Solo controllo degli accessi IAM: con questa opzione, tutti gli utenti dell'account con le autorizzazioni IAM richieste hanno accesso a tutte le risorse del Catalogo dati. Per informazioni su come AWS Glue funziona con IAM, consulta How AWS Glue works with IAM.

  Sulla console Lake Formation, questo metodo ha il nome Usa solo il controllo degli accessi IAM.

> **Note**
>
> Se desideri creare filtri di dati e utilizzare altre funzionalità di Lake Formation, devi utilizzare il controllo degli accessi di Lake Formation.

- Controllo degli accessi di Lake Formation: questo metodo offre i seguenti vantaggi.
  - Puoi implementare la sicurezza a livello di colonna, riga e cella tramite la creazione di filtri di dati. Per ulteriori informazioni, consulta Proteggere i data lake con il controllo degli accessi a livello di riga nella Guida per gli AWS Lake Formation sviluppatori.
  - Il database e le tabelle sono visibili solo agli amministratori di Lake Formation e ai creatori del database e delle risorse di Lake Formation. Se un altro utente deve accedere a queste risorse, devi concedere l'accesso utilizzando le autorizzazioni di Lake Formation in modo esplicito.

Per ulteriori informazioni sul controllo granulare degli accessi, consulta Metodi per il controllo granulare degli accessi.

Determinazione del metodo di autorizzazione per una risorsa federata

Quando abiliti la federazione per la prima volta, CloudTrail crea un database gestito e una tabella federata gestita utilizzando le impostazioni del data lake Lake Formation.

Dopo aver CloudTrail abilitato la federazione, puoi verificare quale metodo di autorizzazioni stai utilizzando per il database gestito e la tabella federata gestita controllando le autorizzazioni per tali risorse. Se per la risorsa è presente l'impostazione `ALL` (Super) per `IAM_ALLOWED_PRINCIPALS` , la risorsa viene gestita esclusivamente dalle autorizzazioni IAM. Se l'impostazione non è presente, la risorsa è gestita dalle autorizzazioni di Lake Formation. Per ulteriori informazioni sulle autorizzazioni di Lake Formation, consulta Documentazione di riferimento sulle autorizzazioni Lake Formation.

Il metodo di autorizzazione per il database e la tabella federata gestiti può essere diverso. Ad esempio, se controlli i valori del database e della tabella, potresti visualizzare i seguenti elementi:

- Per il database, se il valore `ALL` (Super) assegnato a `IAM_ALLOWED_PRINCIPALS` è presente nelle autorizzazioni significa che stai utilizzando solo il controllo degli accessi IAM per il database.
- Per la tabella, se il valore `ALL` (Super) assegnato a `IAM_ALLOWED_PRINCIPALS` non è presente, significa che il controllo degli accessi avviene tramite le autorizzazioni di Lake Formation.

Puoi passare da un metodo di accesso all'altro in qualsiasi momento aggiungendo o rimuovendo `ALL` (Super) all'autorizzazione di `IAM_ALLOWED_PRINCIPALS` su qualsiasi risorsa federata in Lake Formation.

Condivisione tra account tramite Lake Formation

In questa sezione viene descritto come condividere un database e una tabella federata gestiti tra account utilizzando Lake Formation.

Puoi condividere un database gestito tra più account seguendo questi passaggi:

1. Aggiorna la versione per la condivisione dei dati tra account alla versione 4.
2. Rimuovi `Super` dalle autorizzazioni `IAM_ALLOWED_PRINCIPALS` del database, se presenti, per passare al controllo degli accessi di Lake Formation.
3. Concedi autorizzazioni `Describe` all'account esterno sul database.
4. Se una risorsa del Data Catalog è condivisa con te Account AWS e il tuo account non fa parte della stessa AWS organizzazione dell'account di condivisione, accetta l'invito alla condivisione delle risorse da AWS Resource Access Manager (AWS RAM). Per ulteriori informazioni, consulta Accettazione di un invito alla condivisione di risorse dalla AWS RAM.

Dopo aver completato questi passaggi, il database dovrebbe essere visibile all'account esterno. Per impostazione predefinita, la condivisione del database non consente l'accesso ad alcuna tabella presente al suo interno.

Puoi condividere tutte le tabelle federate gestite o tabelle singole con un account esterno seguendo questi passaggi:

1. Aggiorna la versione per la condivisione dei dati tra account alla versione 4.
2. Rimuovi `Super` dalle autorizzazioni `IAM_ALLOWED_PRINCIPALS` della tabella, se presenti, per passare al controllo degli accessi di Lake Formation.
3. (Facoltativo) Specifica eventuali filtri di dati per limitare colonne o righe.
4. Concedi autorizzazioni `Select` all'account esterno sulla tabella.
5. Se una risorsa di Data Catalog è condivisa con il tuo account Account AWS e il tuo account non fa parte della stessa AWS organizzazione dell'account di condivisione, accetta l'invito alla condivisione delle risorse da AWS Resource Access Manager (AWS RAM). Per un'organizzazione, puoi accettare automaticamente l'invito utilizzando le impostazioni RAM. Per

ulteriori informazioni, consulta Accettazione di un invito alla condivisione di risorse dalla AWS RAM.

6. La tabella dovrebbe ora essere visibile. Per abilitare le query di Amazon Athena su questa tabella, crea un link alla risorsa in questo account con la tabella condivisa.

L'account proprietario può revocare la condivisione in qualsiasi momento rimuovendo le autorizzazioni per l'account esterno da Lake Formation o disabilitando la federazione in. CloudTrail

Comprendere gli archivi di dati degli eventi organizzativi

Se è stata creata un'organizzazione in AWS Organizations, è possibile creare un data store di eventi organizzativi che registri tutti Account AWS gli eventi di quell'organizzazione. Gli archivi dati degli eventi organizzativi possono essere applicati a tutti Regioni AWS o alla regione corrente. Non puoi utilizzare un datastore di eventi dell'organizzazione per raccogliere eventi dall'esterno di AWS.

È possibile creare un data store di eventi organizzativi utilizzando l'account di gestione o l'account amministratore delegato. Quando un amministratore delegato crea un datastore di eventi dell'organizzazione, quest'ultimo esiste nell'account di gestione dell'organizzazione. Questo approccio è dovuto al fatto che l'account di gestione mantiene la proprietà di tutte le risorse dell'organizzazione.

L'account di gestione di un'organizzazione può aggiornare un data store di eventi a livello di account per applicarlo a un'organizzazione.

Quando il datastore di eventi dell'organizzazione viene specificato come applicabile a un'organizzazione, viene applicato automaticamente a tutti gli account membri di tale organizzazione. Gli account membri non possono visualizzare il datastore di eventi dell'organizzazione né possono modificarlo o eliminarlo. Per impostazione predefinita, gli account membri non hanno accesso al datastore di eventi dell'organizzazione né possono eseguire query su tali datastore.

La tabella seguente mostra le funzionalità dell'account di gestione e degli account amministratore delegato all'interno dell'organizzazione. AWS Organizations

Funzionalità	Gestione dell'account	Account amministratore delegato
Registrazione o rimozione di account amministratore delegato.	Sì	No

Funzionalità	Gestione dell'account	Account amministratore delegato
Crea un archivio dati degli eventi organizzativi per AWS CloudTrail eventi o elementi AWS Config di configurazione.	Sì	Sì
Abilitazione di Insights in un datastore di eventi dell'organizzazione.	Sì	No
Aggiornamento di un datastore di eventi dell'organizzazione.	Sì	Sì [1]
Avvia e interrompi l'inserimento degli eventi in un archivio dati di eventi organizzativi.	Sì	Sì
Abilitazione della federazione delle query di Data Lake in un datastore di eventi dell'organizzazione.[2]	Sì	Sì
Disabilitazione della federazione delle query di Data Lake in un datastore di eventi dell'organizzazione.	Sì	Sì
Eliminazione di un datastore di eventi dell'organizzazione.	Sì	Sì
Copia di eventi del percorso in un datastore di eventi.	Sì	No
Esecuzione di query sui datastore di eventi dell'organizzazione.	Sì	Sì
Visualizza una dashboard gestita per un data store di eventi organizzativi.	Sì	No
Abilita la dashboard Highlights per gli archivi di dati degli eventi organizzativi.	Sì	No

Funzionalità	Gestione dell'account	Account amministratore delegato
Crea un widget per una dashboard personalizzata che interroga un data store di eventi organizzativi.	Sì	No

[1] Solo l'account di gestione può convertire un data store di eventi organizzativi in un data store di eventi a livello di account o convertire un data store di eventi a livello di account in un data store di eventi organizzativi. Queste operazioni non sono consentite all'amministratore delegato perché i datastore di eventi dell'organizzazione esistono solo nell'account di gestione. Quando un data store di eventi organizzativi viene convertito in un data store di eventi a livello di account, solo l'account di gestione ha accesso al data store degli eventi. Analogamente, solo un data store di eventi a livello di account nell'account di gestione può essere convertito in un data store di eventi dell'organizzazione.

[2]Solo un singolo account amministratore delegato o l'account di gestione può abilitare la federazione in un datastore di eventi dell'organizzazione. Altri account amministratore delegato possono eseguire query e condividere informazioni utilizzando la funzionalità di condivisione dei dati di Lake Formation. Qualsiasi account amministratore delegato, nonché l'account di gestione dell'organizzazione, può disabilitare la federazione.

Crea un data store di eventi organizzativi

L'account di gestione o l'account amministratore delegato di un'organizzazione può creare un data store di eventi organizzativi per raccogliere CloudTrail eventi (eventi di gestione, eventi relativi ai dati) o elementi di AWS Config configurazione.

> **Note**
>
> Solo l'account di gestione dell'organizzazione può copiare gli eventi di trail in un data store di eventi.

CloudTrail console

Per creare un data store di eventi organizzativi utilizzando la console

1. Segui i passaggi della procedura di creazione di un data store di CloudTrail eventi per eventi per creare un data store di eventi organizzativi per la CloudTrail gestione degli eventi o dei dati.

   OPPURE

   Segui i passaggi della procedura di creazione di un data store di eventi per gli elementi di AWS Config configurazione per creare un data store di eventi dell'organizzazione per gli elementi di AWS Config configurazione.
2. Nella pagina Scegli eventi, scegli Abilita per tutti gli account della mia organizzazione.

AWS CLI

Per creare un archivio dati di eventi organizzativi, esegui il create-event-data-storecomando e includi l'`--organization-enabled`opzione.

Il AWS CLI `create-event-data-store` comando di esempio seguente crea un archivio dati di eventi organizzativi che raccoglie tutti gli eventi di gestione. Poiché CloudTrail registra gli eventi di gestione per impostazione predefinita, non è necessario specificare selettori di eventi avanzati se l'Event Data Store registra tutti gli eventi di gestione e non raccoglie alcun evento relativo ai dati.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Il AWS CLI `create-event-data-store` comando di esempio successivo crea un archivio dati di eventi organizzativi denominato `config-items-org-eds` che raccoglie AWS Config gli elementi di configurazione. Per raccogliere gli elementi di configurazione, specificate che il `eventCategory` campo sia uguale `ConfigurationItem` nei selettori di eventi avanzati.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Applica un data store di eventi a livello di account a un'organizzazione

L'account di gestione dell'organizzazione può convertire un data store di eventi a livello di account per applicarlo a un'organizzazione.

CloudTrail console

Per aggiornare un data store di eventi a livello di account utilizzando la console

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione, seleziona Datastore di eventi in Lake.
3. Scegli il datastore di eventi da aggiornare. Questa operazione apre la pagina dei dettagli del datastore di eventi.
4. In General details (Dettagli generali), scegli Edit (Modifica).
5. Scegli Abilita per tutti gli account della mia organizzazione.
6. Scegli Save changes (Salva modifiche).

Per ulteriori informazioni sull'aggiornamento di un archivio dati di eventi, consultaAggiorna un data store di eventi con la console.

AWS CLI

Per aggiornare un Event Data Store a livello di account per applicarlo a un'organizzazione, esegui il update-event-data-storecomando e includi l'`--organization-enabled`opzione.

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Politica delle risorse predefinita per gli amministratori delegati

CloudTrail genera automaticamente una politica delle risorse denominata `DelegatedAdminResourcePolicy` Data Store degli eventi organizzativi che elenca le azioni che gli account amministratore delegati sono autorizzati a eseguire sugli archivi dati degli eventi organizzativi. Le autorizzazioni in `DelegatedAdminResourcePolicy` derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations

Lo scopo di `DelegatedAdminResourcePolicy` è garantire che gli account amministratore delegato possano gestire l'archivio dati degli eventi dell'organizzazione per conto dell'organizzazione e non venga negato involontariamente l'accesso all'archivio dati degli eventi dell'organizzazione quando all'archivio dati degli eventi dell'organizzazione è associata una politica basata sulle risorse

che consente o impedisce ai responsabili di eseguire un'azione sull'archivio dati degli eventi dell'organizzazione.

CloudTrail valuta insieme a qualsiasi politica basata `DelegatedAdminResourcePolicy` sulle risorse fornita per l'archivio dati degli eventi dell'organizzazione. L'accesso agli account degli amministratori delegati verrebbe negato solo se la politica basata sulle risorse fornita includesse una dichiarazione che impedisse esplicitamente agli account amministratore delegati di eseguire un'azione sul data store degli eventi organizzativi che gli account amministratore delegati sarebbero altrimenti in grado di eseguire.

Questa politica viene aggiornata automaticamente quando: `DelegatedAdminResourcePolicy`

- L'account di gestione converte un data store di eventi organizzativi in un data store di eventi a livello di account oppure converte un data store di eventi a livello di account in un data store di eventi organizzativi.
- Sono state apportate modifiche all'organizzazione. Ad esempio, l'account di gestione registra o rimuove un account amministratore CloudTrail delegato.

È possibile visualizzare la up-to-date politica nella sezione Politica delle risorse dell'amministratore delegato sulla CloudTrail console oppure eseguendo il AWS CLI `get-resource-policy` comando e passando l'ARN dell'archivio dati degli eventi dell'organizzazione.

L'esempio seguente esegue il `get-resource-policy` comando su un archivio dati di eventi organizzativi.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

L'output di esempio seguente mostra sia la politica basata sulle risorse fornita sia quella `DelegatedAdminResourcePolicy` generata per gli account di amministratore delegato e. `333333333333` `111111111111`

```
{
  "ResourceArn": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207",
  "ResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "EdsPolicyA",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::666666666666:root"
      },
      "Action": [
        "cloudtrail:geteventdatastore",
        "cloudtrail:startquery",
        "cloudtrail:describequery",
        "cloudtrail:cancelquery",
        "cloudtrail:generatequery",
        "cloudtrail:generatequeryresultssummary"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  },
  "DelegatedAdminResourcePolicy": {
    "Version": "2012-10-17",
    "Statement": [{
      "Sid": "Organization-EventDataStore-Auto-Generated-Delegated-Admin-Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["333333333333", "111111111111"]
      },
      "Action": [
        "cloudtrail:AddTags",
        "cloudtrail:CancelQuery",
        "cloudtrail:CreateEventDataStore",
        "cloudtrail:DeleteEventDataStore",
        "cloudtrail:DescribeQuery",
        "cloudtrail:DisableFederation",
        "cloudtrail:EnableFederation",
        "cloudtrail:GenerateQuery",
        "cloudtrail:GenerateQueryResultsSummary",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListQueries",
        "cloudtrail:ListTags",
        "cloudtrail:RemoveTags",
        "cloudtrail:RestoreEventDataStore",
        "cloudtrail:UpdateEventDataStore",
```

```
        "cloudtrail:StartEventDataStoreIngestion",
        "cloudtrail:StartQuery",
        "cloudtrail:StopEventDataStoreIngestion",
        "cloudtrail:UpdateEventDataStore"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-
d493-4914-9182-e52a7934b207"
    }]
  }
}
```

Risorse aggiuntive

- Amministratori delegati dell'organizzazione
- Aggiunta di un CloudTrail amministratore delegato
- Rimozione di un CloudTrail amministratore delegato

Crea un'integrazione con una fonte di eventi esterna a AWS

Puoi utilizzarli CloudTrail per registrare e archiviare i dati sulle attività degli utenti da qualsiasi fonte nei tuoi ambienti ibridi, come applicazioni interne o SaaS ospitate in locale o nel cloud, macchine virtuali o contenitori. Puoi archiviare e analizzare questi dati, accedervi, risolverne i problemi e intervenire su di essi senza dover gestire diversi aggregatori di log e strumenti di reportistica.

Gli eventi di attività provenienti da AWS fonti diverse funzionano utilizzando i canali per portare eventi in CloudTrail Lake da partner esterni che collaborano con CloudTrail o provenienti da fonti proprie. Quando crei un canale, scegli uno o più archivi di dati degli eventi per archiviare gli eventi che provengono dall'origine del canale. È possibile modificare gli archivi di dati degli eventi di destinazione per un canale in base alle esigenze, a condizione che tali archivi siano impostati per registrare gli eventi `eventCategory="ActivityAuditLog"`. Quando crei un canale per gli eventi provenienti da un partner esterno, fornisci un ARN di canale al partner o all'applicazione di origine. La policy delle risorse collegata al canale consente all'origine di trasmettere eventi attraverso il canale. Se un canale non dispone di una policy delle risorse, solo il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale.

CloudTrail ha collaborato con molti fornitori di fonti di eventi, come Okta e. LaunchDarkly Quando crei un'integrazione con una fonte di eventi esterna AWS, puoi scegliere uno di questi partner come fonte

di eventi o scegliere La mia integrazione personalizzata in cui integrare gli eventi provenienti dalle tue fonti. CloudTrail È consentito un massimo di un canale per origine.

Esistono due tipi di integrazione: diretta e soluzione. Con le integrazioni dirette, il partner chiama l'`PutAuditEvents`API per inviare eventi all'archivio dati degli eventi relativo al tuo AWS account. Con le integrazioni di soluzioni, l'applicazione viene eseguita nell' AWS account dell'utente e richiama l'`PutAuditEvents`API per inviare gli eventi all'archivio dati degli eventi relativo all'account AWS .

Dalla pagina Integrations (Integrazioni), puoi scegliere la scheda Available sources (Origini disponibili) per visualizzare l'Integration type (Tipo di integrazione) dei partner.

Per iniziare, crea un'integrazione per registrare gli eventi dai partner o da altre fonti applicative utilizzando la CloudTrail console.

Argomenti

- Crea un'integrazione con un CloudTrail partner tramite la console
- Crea un'integrazione personalizzata con la console
- Crea, aggiorna e gestisci le integrazioni di CloudTrail Lake con AWS CLI
- Ulteriori informazioni sui partner di integrazione
- CloudTrail Schema degli eventi di Lake Integrations

Crea un'integrazione con un CloudTrail partner tramite la console

Quando crei un'integrazione con una fonte di eventi esterna AWS, puoi scegliere uno di questi partner come fonte di eventi. Quando crei un'integrazione CloudTrail con un'applicazione partner, il partner ha bisogno dell'Amazon Resource Name (ARN) del canale che crei in questo flusso di lavoro a cui inviare eventi. CloudTrail Dopo aver creato l'integrazione, completa la configurazione dell'integrazione seguendo le istruzioni del partner per fornire l'ARN di canale richiesto al partner. L'integrazione inizia a importare gli eventi dei partner CloudTrail dopo che il partner ha effettuato le chiamate `PutAuditEvents` sul canale di integrazione.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Dal pannello di navigazione, in Lake, scegli Integrazioni.

3. Nella pagina Add integration (Aggiungi integrazione), inserisci un nome per il tuo canale. Il nome può contenere da 3 a 128 caratteri. Sono consentiti soltanto lettere, numeri, punti, e caratteri di sottolineatura e trattini.
4. Scegli l'origine dell'applicazione del partner dalla quale desideri ottenere gli eventi. Se stai eseguendo l'integrazione con gli eventi delle tue applicazioni ospitate on-premise o nel cloud, scegli My custom integration (La mia integrazione personalizzata).
5. In Event delivery location (Luogo di distribuzione dell'evento), puoi scegliere se registrare gli stessi eventi delle attività negli archivi di dati degli eventi esistenti oppure creare un nuovo archivio di dati degli eventi.

   Se scegli di creare un nuovo datastore di eventi, inserisci un nome per tale datastore, scegli l'opzione di prezzo e specifica il periodo di conservazione in giorni. L'archivio di dati degli eventi conserva i dati degli eventi per il numero specificato di giorni.

   Se scegli di registrare gli eventi delle attività in uno o più archivi di dati degli eventi esistenti, scegli tali archivi dall'elenco. Gli archivi di dati degli eventi possono includere solo eventi delle attività. Il tipo di evento nella console deve essere Events from integrations (Eventi dalle integrazioni). Nell'API, il valore `eventCategory` deve essere `ActivityAuditLog`.
6. In Resource policy (Policy delle risorse), configura la policy delle risorse per il canale dell'integrazione. Le policy delle risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un principale specificato sulla risorsa e in base a quali condizioni. Gli account definiti come principali nella policy delle risorse possono chiamare l'API `PutAuditEvents` per distribuire gli eventi al tuo canale. Il proprietario della risorsa ha accesso implicito alla risorsa se la sua policy IAM consente l'operazione `cloudtrail-data:PutAuditEvents`.

   Le informazioni richieste per la policy dipendono dal tipo di integrazione. Per un'integrazione diretta, aggiunge CloudTrail automaticamente l' AWS account IDs del partner e richiede l'immissione dell'ID esterno univoco fornito dal partner. Per l'integrazione di una soluzione, è necessario specificare almeno un ID AWS account come principale e, facoltativamente, inserire un ID esterno per evitare confusioni.

   > **Note**
   >
   > Se non crei una policy delle risorse per il canale, solo il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale.

a. Per un'integrazione diretta, inserisci l'ID esterno fornito dal partner. Il partner di integrazione fornisce un ID esterno univoco, come un ID account o una stringa generata casualmente, da utilizzare per evitare che l'integrazione incorra nel problema "confused deputy". Il partner ha la responsabilità di creare e fornire un ID esterno univoco.

   Per consultare la documentazione del partner che descrive come trovare l'ID esterno, scegli How to find this? (Come trovarlo?).

   > **Note**
   >
   > Se la policy delle risorse include un ID esterno, tutte le chiamate all'API `PutAuditEvents` devono includere tale ID. Tuttavia, se la policy non definisce un ID esterno, il partner può comunque chiamare l'API `PutAuditEvents` e specificare un parametro `externalId`.

b. Per un'integrazione con una soluzione, scegli Aggiungi AWS account per specificare un ID AWS account da aggiungere come principale nella politica.

7. (Opzionale) Nella sezione Tags (Tag), è possibile aggiungere fino a 50 coppie di chiavi e valori di tag per aiutare a identificare, ordinare e controllare l'accesso al canale e all'archivio di dati degli eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Taggare AWS le risorse in. Riferimenti generali di AWS

8. Quando è tutto pronto per creare la nuova integrazione, scegli Add integration (Aggiungi integrazione). Non esiste una pagina di recensione. CloudTrail crea l'integrazione, ma devi fornire il canale Amazon Resource Name (ARN) all'applicazione partner. Le istruzioni per fornire l'ARN del canale all'applicazione del partner sono disponibili sul sito Web della documentazione dei partner. Per ulteriori informazioni, seleziona il link Learn more (Ulteriori informazioni) relativo al partner nella scheda Available sources (Origini disponibili) della pagina Integrations (Integrazioni) per aprire la pagina del partner in Marketplace AWS.

Per completare la configurazione dell'integrazione, fornisci l'ARN del canale al partner o all'applicazione di origine. A seconda del tipo di integrazione, tu, il partner o l'applicazione eseguite l'API `PutAuditEvents` per distribuire gli eventi dell'attività all'archivio di dati degli

eventi del tuo account AWS . Dopo la pubblicazione degli eventi relativi alle attività, puoi utilizzare CloudTrail Lake per cercare, interrogare e analizzare i dati registrati dalle tue applicazioni. I dati degli eventi includono campi che corrispondono al payload CloudTrail degli eventi, ad esempio `eventVersioneventSource`, e. `userIdentity`

Crea un'integrazione personalizzata con la console

Puoi utilizzarli CloudTrail per registrare e archiviare i dati sulle attività degli utenti da qualsiasi fonte nei tuoi ambienti ibridi, come applicazioni interne o SaaS ospitate in locale o nel cloud, macchine virtuali o contenitori. Esegui la prima metà di questa procedura nella console CloudTrail Lake, quindi chiama l'`PutAuditEvents`API per importare gli eventi, fornendo l'ARN del canale e il payload degli eventi. Dopo aver utilizzato l'`PutAuditEvents`API per importare l'attività dell'applicazione CloudTrail, puoi utilizzare CloudTrail Lake per cercare, interrogare e analizzare i dati registrati dalle tue applicazioni.

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Dal pannello di navigazione, in Lake, scegli Integrazioni.
3. Nella pagina Add integration (Aggiungi integrazione), inserisci un nome per il tuo canale. Il nome può contenere da 3 a 128 caratteri. Sono consentiti soltanto lettere, numeri, punti, e caratteri di sottolineatura e trattini.
4. Scegli My custom integration (La mia integrazione personalizzata).
5. In Event delivery location (Luogo di distribuzione dell'evento), puoi scegliere se registrare gli stessi eventi delle attività negli archivi di dati degli eventi esistenti oppure creare un nuovo archivio di dati degli eventi.

   Se scegli di creare un nuovo archivio di dati degli eventi, inserisci un nome per tale archivio e specifica il periodo di conservazione in giorni. Puoi conservare i dati degli eventi in un datastore di eventi per un massimo di 3.653 giorni (circa 10 anni) se scegli l'opzione Prezzo per la conservazione estendibile di un anno o di 2.557 giorni (circa 7 anni) se scegli l'opzione Prezzo per la conservazione di sette anni.

   Se scegli di registrare gli eventi delle attività in uno o più archivi di dati degli eventi esistenti, scegli tali archivi dall'elenco. Gli archivi di dati degli eventi possono includere solo eventi delle attività. Il tipo di evento nella console deve essere Events from integrations (Eventi dalle integrazioni). Nell'API, il valore `eventCategory` deve essere `ActivityAuditLog`.

6. In Resource policy (Policy delle risorse), configura la policy delle risorse per il canale dell'integrazione. Le policy delle risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un principale specificato sulla risorsa e in base a quali condizioni. Gli account definiti come principali nella policy delle risorse possono chiamare l'API `PutAuditEvents` per distribuire gli eventi al tuo canale.

   > **Note**
   >
   > Se non crei una policy delle risorse per il canale, solo il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale.

   a. (Facoltativo) Inserisci un ID esterno univoco per aggiungere un ulteriore livello di protezione. L'ID esterno univoco è una stringa univoca, come un ID account o una stringa generata casualmente, che evita il problema "confused deputy".

      > **Note**
      >
      > Se la policy delle risorse include un ID esterno, tutte le chiamate all'API `PutAuditEvents` devono includere tale ID. Tuttavia, se la policy non definisce un ID esterno, puoi comunque chiamare l'API `PutAuditEvents` e specificare un parametro `externalId`.

   b. Scegli Aggiungi AWS account per specificare l'ID di ogni AWS account da aggiungere come principale nella politica delle risorse del canale.

7. (Opzionale) Nella sezione Tags (Tag), è possibile aggiungere fino a 50 coppie di chiavi e valori di tag per aiutare a identificare, ordinare e controllare l'accesso al canale e all'archivio di dati degli eventi. Per ulteriori informazioni su come utilizzare le policy IAM per autorizzare l'accesso a un archivio di dati degli eventi in base ai tag, consultare Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Taggare le AWS risorse in. Riferimenti generali di AWS

8. Quando è tutto pronto per creare la nuova integrazione, scegli Add integration (Aggiungi integrazione). Non esiste una pagina di recensione. CloudTrail crea l'integrazione, ma per integrare i tuoi eventi personalizzati, devi specificare l'ARN del canale in una `PutAuditEvents`richiesta.

9. Chiama l'`PutAuditEvents`API per inserire i tuoi eventi di attività. CloudTrail Puoi aggiungere fino a 100 eventi delle attività (o fino a 1 MB) per ciascuna richiesta `PutAuditEvents`. Avrai

bisogno dell'ARN del canale che hai creato nei passaggi precedenti, del payload di eventi che desideri CloudTrail aggiungere e dell'ID esterno (se specificato per la tua politica delle risorse). Assicurati che nel payload dell'evento non siano presenti informazioni sensibili o che consentano l'identificazione personale prima di inserirle. CloudTrail Gli eventi in cui immetti devono seguire il. CloudTrail CloudTrail Schema degli eventi di Lake Integrations

> **Tip**
>
> AWS CloudShellUtilizzatelo per assicurarvi di utilizzare la versione più aggiornata AWS APIs.

Negli esempi seguenti viene illustrato come utilizzare il comando CLI put-audit-events. I parametri --audit-events e --channel-arn sono obbligatori. È necessario fornire l'ARN del canale creato nei passaggi precedenti, che puoi copiare dalla pagina dei dettagli dell'integrazione. Il valore di --audit-events è una matrice JSON di oggetti evento. `--audit-events`include un ID richiesto dall'evento, il payload richiesto dell'evento come valore di `EventData` e un checksum opzionale per convalidare l'integrità dell'evento dopo l'ingestione in. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

Di seguito è riportato un comando di esempio con due esempi di eventi.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Il seguente comando di esempio aggiunge il parametro `--cli-input-json` per specificare un file JSON (`custom-events.json`) del payload dell'evento.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

I seguenti sono i contenuti di esempio del file JSON di esempio, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(Facoltativo) Calcolo di un valore di checksum

Il checksum specificato come valore di una `PutAuditEvents` richiesta consente di `EventDataChecksum` verificare la CloudTrail ricezione dell'evento corrispondente al checksum; aiuta a verificare l'integrità degli eventi. Il valore di checksum è un SHA256 algoritmo base64 che si calcola eseguendo il comando seguente.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
```

```
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

Il comando restituisce il checksum. Di seguito è riportato un esempio.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

Il valore del checksum diventa il valore di `EventDataChecksum` nella richiesta `PutAuditEvents`. Se il checksum non corrisponde a quello dell'evento fornito, CloudTrail rifiuta l'evento con un errore. `InvalidChecksum`

Crea, aggiorna e gestisci le integrazioni di CloudTrail Lake con AWS CLI

Questa sezione descrive i comandi che puoi utilizzare per creare, aggiornare e gestire le tue integrazioni CloudTrail Lake utilizzando. AWS CLI

Quando usi il AWS CLI, ricorda che i tuoi comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Comandi disponibili per le integrazioni con CloudTrail Lake

I comandi per creare, aggiornare e gestire le integrazioni in CloudTrail Lake includono:

- `create-event-data-store`per creare un archivio dati di eventi per eventi esterni a. AWS
- `delete-channel`per eliminare un canale utilizzato per un'integrazione.
- `delete-resource-policy`per eliminare la politica delle risorse allegata a un canale per un'integrazione con CloudTrail Lake.
- `get-channel`per restituire informazioni su un CloudTrail canale.
- `get-resource-policy`per recuperare il testo JSON del documento di policy basato sulle risorse allegato al canale. CloudTrail
- `list-channels`per elencare i canali nell'account corrente e i relativi nomi di origine.

- `put-audit-events`per importare gli eventi della tua applicazione in CloudTrail Lake. Un parametro obbligatorio`auditEvents`, accetta i record JSON (chiamati anche payload) degli eventi che si desidera CloudTrail importare. Puoi aggiungere fino a 100 di questi eventi (o fino a 1 MB) per richiesta. `PutAuditEvents`
- `put-resource-policy`per allegare una politica di autorizzazione basata sulle risorse a un CloudTrail canale utilizzato per l'integrazione con una fonte di eventi esterna a. AWSPer ulteriori informazioni sulle politiche basate sulle risorse, consulta esempi di policy basate sulle risorse.AWS CloudTrail
- `update-channel`per aggiornare un canale specificato da un ARN o UUID del canale richiesto.

Per un elenco dei comandi disponibili per i data store di eventi CloudTrail Lake, vedi. Comandi disponibili per gli archivi dati degli eventi

Per un elenco dei comandi disponibili per le query CloudTrail Lake, consultaComandi disponibili per le query su CloudTrail Lake.

Per un elenco dei comandi disponibili per le dashboard di CloudTrail Lake, consulta. Comandi disponibili per i dashboard

Crea un'integrazione per registrare gli eventi dall'esterno AWS con AWS CLI

Questa sezione descrive come utilizzare AWS CLI per creare un'integrazione CloudTrail Lake per registrare eventi dall'esterno di AWS.

In AWS CLI, crei un'integrazione in quattro comandi (tre se disponi già di un archivio dati di eventi che soddisfa i criteri). I data store di eventi utilizzati come destinazioni per un'integrazione devono essere per una singola regione e un singolo account; non possono essere multiregionali, non possono registrare eventi per le organizzazioni e possono includere solo eventi di attività. AWS Organizations Il tipo di evento nella console deve essere Events from integrations (Eventi dalle integrazioni). Nell'API, il valore `eventCategory` deve essere `ActivityAuditLog`. Per ulteriori informazioni sulle integrazioni, consulta la pagina Crea un'integrazione con una fonte di eventi esterna a AWS.

1. Esegui create-event-data-store per creare un archivio di dati degli eventi, se non disponi già di uno o più archivi di dati degli eventi da utilizzare per l'integrazione.

   Il AWS CLI comando di esempio seguente crea un archivio dati di eventi che registra gli eventi dall'esterno. AWS Per gli eventi delle attività, il valore del selettore del campo `eventCategory` è `ActivityAuditLog`. L'archivio di dati degli eventi ha un periodo di conservazione di 90

giorni. Per impostazione predefinita, l'event data store raccoglie eventi da tutte le regioni, ma poiché raccoglie AWS eventi diversi, impostalo su una singola regione aggiungendo l'`--no-multi-region-enabled`opzione. La protezione dalla terminazione è abilitata per impostazione predefinita e l'archivio di dati degli eventi non raccoglie eventi per gli account di un'organizzazione.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--no-multi-region-enabled \
--retention-period 90 \
--advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Avrai bisogno dell'ID dell'archivio di dati degli eventi (il suffisso dell'ARN o `EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE` nell'esempio di risposta precedente) per andare al passaggio successivo e creare il tuo canale.

2. Esegui il create-channelcomando per creare un canale che consenta a un'applicazione partner o sorgente di inviare eventi a un archivio dati di eventi in CloudTrail.

   Un canale include i seguenti componenti:

   Origine

   CloudTrail utilizza queste informazioni per determinare i partner a cui inviano i dati degli eventi per CloudTrail conto dell'utente. È necessaria un'origine, che può essere `Custom` per tutti gli eventi esterni ad AWS validi o il nome di un'origine di eventi del partner. È consentito un massimo di un canale per origine.

   Per informazioni sui valori di `Source` dei partner disponibili, consulta la pagina Ulteriori informazioni sui partner di integrazione.

   Stato di importazione

   Lo stato del canale mostra quando sono stati ricevuti gli ultimi eventi da un'origine del canale.

   Destinazioni

   Le destinazioni sono gli archivi di dati degli eventi CloudTrail Lake che ricevono eventi dal canale. È possibile modificare gli archivi di dati degli eventi di destinazione per un canale.

   Per interrompere la ricezione di eventi da un'origine, elimina il rispettivo canale.

   È necessario specificare l'ID di almeno un archivio di dati degli eventi di destinazione per eseguire questo comando. Il tipo di destinazione valido è `EVENT_DATA_STORE`. È possibile inviare gli eventi importati a più di un archivio di dati degli eventi. Il comando di esempio seguente crea un canale che invia eventi a due archivi di dati di eventi, rappresentati da essi IDs nell'`Location`attributo del `--destinations` parametro. I parametri `--destinations`, `--name` e `--source` sono obbligatori. Per importare eventi da un CloudTrail partner, specificate

il nome del partner come valore di`--source`. Per importare eventi dalle vostre applicazioni all'esterno AWS, specificate `Custom` come valore di. `--source`

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

Nella risposta al comando create-channel, copia l'ARN del nuovo canale. Per eseguire i comandi `put-resource-policy` e `put-audit-events` nei passaggi successivi è necessario l'ARN.

3. Eseguite il put-resource-policycomando per allegare una politica delle risorse al canale. Le policy delle risorse sono documenti di policy JSON che specificano le operazioni che possono essere eseguite da un principale specificato sulla risorsa e in base a quali condizioni. Gli account definiti come principali nella policy delle risorse del canale possono chiamare l'API `PutAuditEvents` per distribuire gli eventi.

> **Note**
>
> Se non crei una policy delle risorse per il canale, solo il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale.

Le informazioni richieste per la policy dipendono dal tipo di integrazione.

- Per un'integrazione direzionale, CloudTrail richiede che la policy contenga l' AWS account IDs del partner e richiede l'immissione dell'ID esterno univoco fornito dal partner. CloudTrail aggiunge automaticamente l' AWS account del partner IDs alla politica delle risorse quando si crea un'integrazione utilizzando la CloudTrail console. Consulta la documentazione del partner per scoprire come ottenere i numeri di AWS account necessari per la policy.
- Per l'integrazione di una soluzione, è necessario specificare almeno un ID AWS account come principale e, facoltativamente, inserire un ID esterno per evitare di creare confusione tra deputati.

Di seguito sono riportati i requisiti per la policy delle risorse:

- L'ARN della risorsa definito nella policy deve corrispondere all'ARN del canale al quale è collegata la policy.
- La policy contiene una sola azione: cloudtrail-data: PutAuditEvents
- La policy deve includere almeno un'istruzione. La policy può avere un massimo di 20 istruzioni.
- Ogni istruzione contiene almeno un principale. Un'istruzione può avere un massimo di 50 principali.

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

Per ulteriori informazioni sulle policy delle risorse, consulta AWS CloudTrail esempi di policy basate sulle risorse.

4. Esegui l'`PutAuditEvents`API in cui inserire gli eventi delle tue attività. CloudTrail Avrai bisogno del payload di eventi che desideri CloudTrail aggiungere. Assicurati che non vi siano informazioni sensibili o che consentano l'identificazione personale nell'evento payload prima di inserirle. CloudTrail Nota che l'API `PutAuditEvents` utilizza l'endpoint della CLI `cloudtrail-data` anziché l'endpoint `cloudtrail`.

   Negli esempi seguenti viene illustrato come utilizzare il comando CLI put-audit-events. I parametri --audit-events e --channel-arn sono obbligatori. Il parametro --external-id è obbligatorio se nella policy delle risorse è definito un ID esterno. È necessario specificare l'ARN del canale creato nella fase precedente. Il valore di --audit-events è una matrice JSON di oggetti evento. `--audit-events`include un ID richiesto dall'evento, il payload richiesto dell'evento come valore di `EventData` e un checksum opzionale per convalidare l'integrità dell'evento dopo l'ingestione in. CloudTrail

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

   Di seguito è riportato un comando di esempio con due esempi di eventi.

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Il seguente comando di esempio aggiunge il parametro `--cli-input-json` per specificare un file JSON (`custom-events.json`) del payload dell'evento.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

I seguenti sono i contenuti di esempio del file JSON di esempio, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

È possibile verificare che l'integrazione funzioni e che gli eventi vengano CloudTrail importati correttamente dall'origine eseguendo il comando. get-channel L'output di get-channel mostra il timestamp più recente con cui sono stati ricevuti gli CloudTrail eventi.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Facoltativo) Calcolo di un valore di checksum

Il checksum specificato come valore di una `PutAuditEvents` richiesta consente di `EventDataChecksum` verificare che CloudTrail riceva l'evento corrispondente al checksum e di

verificare l'integrità degli eventi. Il valore di checksum è un SHA256 algoritmo base64 che si calcola eseguendo il comando seguente.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

Il comando restituisce il checksum. Di seguito è riportato un esempio.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

Il valore del checksum diventa il valore di `EventDataChecksum` nella richiesta `PutAuditEvents`. Se il checksum non corrisponde a quello dell'evento fornito, CloudTrail rifiuta l'evento con un errore. `InvalidChecksum`

Aggiorna un canale con AWS CLI

Questa sezione descrive come utilizzare il AWS CLI per aggiornare un canale per un'integrazione CloudTrail Lake. È possibile eseguire il `update-channel` comando per aggiornare il nome del canale o per specificare un data store di eventi di destinazione diverso. Non è possibile modificare l'origine di un canale.

Quando si esegue il comando, il `--channel` parametro è obbligatorio.

Di seguito è riportato un esempio che dimostra come aggiornare il nome e la destinazione del canale.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
```

```
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

Eliminare un canale per eliminare un'integrazione con AWS CLI

Questa sezione descrive come eseguire il `delete-channel` comando per eliminare il canale per un'integrazione CloudTrail Lake. È necessario eliminare un canale se si desidera interrompere l'acquisizione di partner o altre attività al di fuori di. AWSÈ necessario specificare l'ARN o l'ID del canale (il suffisso ARN) del canale che desideri eliminare.

L'esempio seguente mostra come eliminare il canale.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Ulteriori informazioni sui partner di integrazione

La tabella in questa sezione fornisce il nome di origine per ogni partner di integrazione e identifica il tipo di integrazione (diretta o di soluzione).

Le informazioni nella colonna Source name (Nome dell'origine) sono necessarie quando si chiama l'API `CreateChannel`. Specifica il nome dell'origine come valore del parametro `Source`.

Nome del partner (console)	Nome dell'origine (API)	Tipo di integrazione
La mia integrazione personalizzata	`Custom`	soluzione
Sicurezza dell'archiviazione nel cloud	`CloudStorageSecurityConsole`	soluzione
Clumio	`Clumio`	diretta
CrowdStrike	`CrowdStrike`	soluzione
CyberArk	`CyberArk`	soluzione
GitHub	`GitHub`	soluzione

Nome del partner (console)	Nome dell'origine (API)	Tipo di integrazione
Kong Inc	`KongGatewayEnterprise`	soluzione
LaunchDarkly	`LaunchDarkly`	diretta
Netskope	`NetskopeCloudExchange`	soluzione
Nordcloud, una società IBM	`IBMMulticloud`	diretta
MontyCloud	`MontyCloud`	diretta
Okta	`OktaSystemLogEvents`	soluzione
One Identity	`OneLogin`	soluzione
Shoreline.io	`Shoreline`	soluzione
Snyk.io	`Snyk`	diretta
Wiz	`WizAuditLogs`	soluzione

Visualizzazione della documentazione dei partner

Puoi saperne di più sull'integrazione di un partner con CloudTrail Lake consultando la relativa documentazione.

Visualizzazione della documentazione dei partner

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, in Lake, scegli Integrazioni.
3. Nella pagina Integrations (Integrazioni), scegli Available sources (Origini disponibili), quindi scegli Learn more (Ulteriori informazioni) relativamente al partner di cui desideri visualizzare la documentazione.

CloudTrail Schema degli eventi di Lake Integrations

La tabella seguente descrive gli elementi dello schema obbligatori e facoltativi che corrispondono a quelli presenti nei record CloudTrail degli eventi. I contenuti di `eventData` sono forniti dai tuoi eventi; gli altri campi sono forniti da CloudTrail after ingestion.

CloudTrail i contenuti dei record degli eventi sono descritti più dettagliatamente in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete

- Campi forniti da CloudTrail dopo l'ingestione
- Campi forniti dai tuoi eventi

I seguenti campi sono forniti da CloudTrail after ingestion:

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
eventVersion	string	Richiesto	La versione dell'evento.
eventCategory	string	Richiesto	La categoria dell'evento. Per i non AWS eventi, il valore è. `ActivityAuditLog`
eventType	string	Richiesto	Il tipo di evento, Per i non AWS eventi, il valore valido è`ActivityLog` .
eventID	string	Richiesto	Un ID univoco per un evento.
eventTime	string	Richiesto	Il timestamp dell'evento, in formato `yyyy-MM-DDTHH:mm:ss` , espresso in tempo

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
			coordinato universale (UTC).
awsRegion	string	Richiesto	Il Regione AWS luogo in cui è stata effettuata la `PutAuditEvents` chiamata.
recipientAccountId	string	Richiesto	Rappresenta l'ID dell'account che ha ricevuto questo evento. CloudTrail compila questo campo calcolandolo dal payload dell'evento.
addendum	-	Facoltativo	Mostra informazioni sul motivo per cui l'elaborazione di un evento è stata ritardata. Se mancavano informazioni da un evento esistente, il blocco aggiuntivo includerà le informazioni mancanti e un motivo per cui mancavano.
• motivo	string	Facoltativo	Il motivo per cui l'evento o alcuni dei suoi contenuti mancavano.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• updatedFields	string	Facoltativo	I campi record di evento aggiornati dall'addendum. Questo è fornito solo se il motivo è `UPDATED_DATA`.
• originalUID	string	Facoltativo	L'UID dell'evento originale dall'origine. Questo è fornito solo se il motivo è `UPDATED_DATA`.
• originalEventID	string	Facoltativo	L'ID evento originale. Questo è fornito solo se il motivo è `UPDATED_DATA`.
metadata	-	Richiesto	Informazioni sul canale utilizzato dall'evento.
• ingestionTime	string	Richiesto	Il timestamp dell'elaborazione dell'evento, in formato `yyyy-MM-DDTHH:mm:ss`, espresso in tempo coordinato universale (UTC).
• channelARN	string	Richiesto	L'ARN del canale utilizzato dall'evento.

I seguenti campi sono forniti dagli eventi dei clienti:

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
eventData	-	Richiesto	I dati di controllo inviati CloudTrai l durante una `PutAuditEvents` chiamata.
• version	string	Richiesto	La versione dell'even to dalla sua origine. Limitazioni di lunghezza: massimo 256 caratteri.
• userIdentity	-	Richiesto	Informazioni sull'uten te che ha effettuato una richiesta.
• • tipo	string	Richiesto	Il tipo di identità utente. Limitazioni di lunghezza: lunghezza massima di 128.
• • principalId	string	Richiesto	Un identificatore univoco per l'attore di un evento. Limitazioni di lunghezza: massimo 1.024 caratteri.
• • details	Oggetto JSON	Facoltativo	Ulteriori informazioni sull'identità.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• userAgent	string	Facoltativo	L'agente tramite il quale è stata effettuat a la richiesta. Limitazioni di lunghezza: massimo 1.024 caratteri.
• eventSource	string	Richiesto	Questa è l'origine dell'evento del partner o l'applicazione personalizzata per la quale vengono registrati gli eventi. Limitazioni di lunghezza: massimo 1.024 caratteri.
• eventName	string	Richiesto	L'operazione richiesta , una delle operazioni nell'API per il servizio o l'applicazione di origine. Limitazioni di lunghezza: massimo 1.024 caratteri.
• eventTime	string	Richiesto	Il timestamp dell'even to, in formato `yyyy-MM-DDTHH:mm:ss` , espresso in tempo coordinato universale (UTC).

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• UID	string	Richiesto	Il valore UID che identifica la richiesta . Questo valore è generato dal servizio o dall'applicazione chiamati. Limitazioni di lunghezza: massimo 1.024 caratteri.
• requestParameters	Oggetto JSON	Facoltativo	Eventuali parametri stati inviati assieme alla richiesta. Questo campo ha una dimensione massima di 100 kB e il contenuto che supera tale limite viene respinto.
• responseElements	Oggetto JSON	Facoltativo	Elemento di risposta per le operazion i che comportano modifiche (operazio ni di creazione , aggiornamento o eliminazione). Questo campo ha una dimensione massima di 100 kB e il contenuto che supera tale limite viene respinto.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• errorCode	string	Facoltativo	Una stringa che rappresenta un errore per l'evento. Limitazioni di lunghezza: massimo 256 caratteri.
• errorMessage	string	Facoltativo	La descrizione dell'errore. Limitazioni di lunghezza: massimo 256 caratteri.
• fonte IPAddress	string	Facoltativo	Indirizzo IP dal quale è stata effettuata la richiesta. Entrambi IPv4 gli IPv6 indirizzi sono accettati.
• recipientAccountId	string	Richiesto	Rappresenta l'ID dell'account che ha ricevuto questo evento. L'ID dell'acco unt deve essere lo stesso dell'ID AWS dell'account proprieta rio del canale.

Nome del campo	Input type (Tipo input)	Requisito	Descrizione
• additionalEventData	Oggetto JSON	Facoltativo	Dati aggiuntivi sull'evento non facenti parte della richiesta o della risposta. Questo campo ha una dimensione massima di 28 kB e il contenuto che supera tale limite viene respinto.

L'esempio seguente mostra la gerarchia degli elementi dello schema che corrispondono a quelli presenti nei record CloudTrail degli eventi.

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
             JSON
```

```
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

CloudTrail Cruscotti Lake

Puoi utilizzare le dashboard di CloudTrail Lake per visualizzare le tendenze degli eventi per gli archivi di dati sugli eventi presenti nel tuo account. CloudTrail Lake offre i seguenti tipi di dashboard:

- Dashboard gestiti: puoi visualizzare una dashboard gestita per visualizzare le tendenze degli eventi per un data store di eventi che raccoglie eventi di gestione, eventi relativi ai dati o eventi Insights. Queste dashboard sono automaticamente disponibili per te e sono gestite da Lake. CloudTrail CloudTrail offre 14 dashboard gestite tra cui scegliere. Puoi aggiornare manualmente i dashboard gestiti. Non è possibile modificare, aggiungere o rimuovere i widget per questi dashboard, tuttavia, è possibile salvare un dashboard gestito come dashboard personalizzato se si desidera modificare i widget o impostare una pianificazione di aggiornamento.
- Dashboard personalizzati: i dashboard personalizzati consentono di interrogare gli eventi in qualsiasi tipo di archivio dati di eventi. Puoi aggiungere fino a 10 widget a una dashboard personalizzata. Puoi aggiornare manualmente una dashboard personalizzata oppure impostare una pianificazione di aggiornamento.

- Dashboard Highlights: abilita la dashboard Highlights per visualizzare una at-a-glance panoramica dell' AWS attività raccolta dagli archivi di dati sugli eventi presenti nel tuo account. La dashboard Highlights è gestita CloudTrail e include widget pertinenti al tuo account. I widget mostrati nella dashboard Highlights sono unici per ogni account. Questi widget potrebbero far emergere attività o anomalie rilevate. Ad esempio, la dashboard Highlights potrebbe includere il widget Total cross-account access, che mostra se c'è un aumento delle attività anomale tra account. CloudTrail aggiorna la dashboard Highlights ogni 6 ore. La dashboard mostra i dati delle ultime 24 ore dall'ultimo aggiornamento.

Ogni dashboard è composta da uno o più widget e ogni widget fornisce una rappresentazione grafica dei risultati di una query SQL. Per visualizzare la query per un widget, scegli Visualizza e modifica interrogazione per aprire l'editor delle query.

Quando una dashboard viene aggiornata, CloudTrail Lake esegue delle query per compilare i widget della dashboard. Poiché l'esecuzione delle query comporta dei costi, ti CloudTrail chiede di riconoscere i costi associati all'esecuzione delle query. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi. CloudTrail

Argomenti

- Prerequisiti
- Limitazioni
- Supporto delle Regioni
- Autorizzazioni richieste
- Visualizza una dashboard gestita con la console CloudTrail
- Abilita la dashboard Highlights con la CloudTrail console
- Disattiva la dashboard Highlights con la console CloudTrail
- Crea una dashboard personalizzata con la CloudTrail console
- Imposta una pianificazione di aggiornamento per una dashboard personalizzata con la console CloudTrail
- Disattiva la pianificazione dell'aggiornamento per una dashboard personalizzata con la console CloudTrail
- Modifica la protezione dalla terminazione con la console CloudTrail
- Elimina una dashboard personalizzata con la console CloudTrail
- Crea, aggiorna e gestisci i dashboard con AWS CLI

Prerequisiti

I seguenti prerequisiti si applicano alle dashboard di CloudTrail Lake:

- Per visualizzare e utilizzare le dashboard di Lake, devi creare almeno un archivio dati di eventi CloudTrail Lake. È possibile creare archivi di dati di eventi utilizzando la AWS CLI console o SDKs. Per informazioni sulla creazione di un datastore di eventi utilizzando la console, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console. Per informazioni sulla creazione di un archivio dati di eventi utilizzando il AWS CLI, vedereCrea un data store di eventi con AWS CLI.
- È necessario disporre delle autorizzazioni adeguate per visualizzare, creare, aggiornare e aggiornare i dashboard. Per ulteriori informazioni, consulta Autorizzazioni richieste.

Limitazioni

Le seguenti limitazioni si applicano ai CloudTrail dashboard di Lake:

- Puoi abilitare la dashboard Highlights solo per gli archivi di dati sugli eventi presenti nel tuo account.
- Puoi visualizzare solo i dashboard gestiti per gli archivi di dati sugli eventi esistenti nel tuo account.
- Per i dashboard personalizzati, puoi solo aggiungere widget di esempio o creare nuovi widget per interrogare gli archivi di dati degli eventi esistenti nel tuo account.
- Gli amministratori delegati di un' AWS Organizations organizzazione non possono visualizzare o gestire i dashboard di proprietà dell'account di gestione.

Supporto delle Regioni

Le dashboard di CloudTrail Lake sono supportate Regioni AWS ovunque CloudTrail sia supportato Lake.

Il widget di riepilogo delle attività nella dashboard Highlights è supportato nelle seguenti regioni:

- Regione Asia Pacifico (Tokyo) (ap-northeast-1)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Regione Stati Uniti occidentali (Oregon) (us-west-1)

Tutti gli altri widget sono supportati Regioni AWS ovunque CloudTrail sia supportato Lake.

Per informazioni sulle regioni supportate da CloudTrail Lake, consultaCloudTrail Regioni supportate dai laghi.

Autorizzazioni richieste

Questa sezione descrive le autorizzazioni richieste per i dashboard di CloudTrail Lake e discute due tipi di policy IAM:

- Policy basate sull'identità che consentono di eseguire azioni per creare, gestire ed eliminare dashboard.
- Policy basate sulle risorse che consentono di CloudTrail eseguire interrogazioni sull'archivio dati degli eventi quando la dashboard viene aggiornata ed eseguire aggiornamenti pianificati delle dashboard personalizzate e della dashboard Highlights per conto dell'utente. Quando crei dashboard utilizzando la CloudTrail console, hai la possibilità di allegare policy basate sulle risorse. Puoi anche eseguire il AWS CLI `put-resource-policy`comando per aggiungere una politica basata sulle risorse agli archivi di dati o ai dashboard degli eventi.

Requisiti politici basati sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Per visualizzare e gestire le dashboard di CloudTrail Lake, è necessaria una delle seguenti politiche:

- La policy gestita `CloudTrailFullAccess`.
- La policy gestita `AdministratorAccess`.
- Una politica personalizzata che include una o più delle autorizzazioni specifiche descritte nelle sezioni seguenti.

Argomenti

- Autorizzazioni necessarie per la creazione di dashboard
- Autorizzazioni necessarie per l'aggiornamento dei dashboard
- Autorizzazioni necessarie per l'aggiornamento dei dashboard

Autorizzazioni necessarie per la creazione di dashboard

La seguente politica di esempio fornisce le autorizzazioni minime richieste per la creazione di dashboard. Sostituisci *partitionregion*,*account-id*, e *eds-id* con i valori della tua configurazione.

- `StartQuery`l'autorizzazione è richiesta solo se la richiesta contiene widget. Fornisci `StartQuery` le autorizzazioni per tutti gli archivi di dati degli eventi inclusi in una query di widget.
- `StartDashboardRefresh`l'autorizzazione è richiesta solo se la dashboard ha una pianificazione di aggiornamento.
- Per la dashboard Highlights, il chiamante deve disporre dell'`StartQuery`autorizzazione per tutti gli archivi di dati sugli eventi dell'account.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Autorizzazioni necessarie per l'aggiornamento dei dashboard

La seguente politica di esempio fornisce le autorizzazioni minime richieste per l'aggiornamento dei dashboard. Sostituisci *partitionregion*,*account-id*, e *eds-id* con i valori della tua configurazione.

- `StartQuery`l'autorizzazione è richiesta solo se la richiesta contiene widget. Fornisci `StartQuery` le autorizzazioni per tutti gli archivi di dati degli eventi inclusi in una query di widget.
- `StartDashboardRefresh`l'autorizzazione è richiesta solo se la dashboard ha una pianificazione di aggiornamento.
- Per la dashboard Highlights, il chiamante deve disporre dell'`StartQuery`autorizzazione per tutti gli archivi di dati sugli eventi dell'account.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:UpdateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Autorizzazioni necessarie per l'aggiornamento dei dashboard

La seguente politica di esempio fornisce le autorizzazioni minime richieste per l'aggiornamento dei dashboard. Sostituisci *`partitionregion`*,*`account-id`*,*`dashboard-name`*, e *`eds-id`* con i valori della tua configurazione.

- Per le dashboard personalizzate e le dashboard Highlights, il chiamante deve avere. `cloudtrail:StartDashboardRefresh permissions`

- Per i dashboard gestiti, il chiamante deve disporre dell'`cloudtrail:StartDashboardRefresh`autorizzazione e `cloudtrail:StartQuery` delle autorizzazioni per l'Event Data Store coinvolto nell'aggiornamento.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/dashboard-
name",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Politiche basate sulle risorse per dashboard e archivi di dati di eventi

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse.

Per eseguire interrogazioni su una dashboard durante un aggiornamento manuale o pianificato, devi allegare una policy basata sulle risorse a ogni archivio di dati di eventi associato a un widget sulla dashboard. Ciò consente a CloudTrail Lake di eseguire le query per tuo conto. Quando crei una dashboard personalizzata o abiliti la dashboard Highlights utilizzando la CloudTrail console, CloudTrail hai la possibilità di scegliere a quali archivi di dati di eventi desideri applicare

le autorizzazioni. Per ulteriori informazioni sulla politica basata sulle risorse, consulta. Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard

Per impostare una pianificazione di aggiornamento per una dashboard, devi allegare alla dashboard una policy basata sulle risorse per consentire a CloudTrail Lake di aggiornare la dashboard per tuo conto. Quando imposti una pianificazione di aggiornamento per una dashboard personalizzata o abiliti la dashboard Highlights utilizzando la CloudTrail console, CloudTrail hai la possibilità di allegare una policy basata sulle risorse alla dashboard. Per un esempio di policy, consulta Esempio di policy basata sulle risorse per un pannello di controllo.

Puoi allegare una policy basata sulle risorse utilizzando la CloudTrail console, l'operazione o l'API. AWS CLIPutResourcePolicy

Autorizzazioni chiave KMS per decrittografare i dati in un archivio dati di eventi

Se un data store di eventi oggetto di una query è crittografato con una chiave KMS, assicurati che la politica delle chiavi KMS CloudTrail consenta di decrittografare i dati nell'archivio dati degli eventi. La seguente dichiarazione politica di esempio consente al responsabile del CloudTrail servizio di decrittografare l'archivio dati degli eventi.

```
{
      "Sid": "AllowCloudTrailDecryptAccess",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Visualizza una dashboard gestita con la console CloudTrail

CloudTrail Lake fornisce dashboard gestite che mostrano le tendenze degli eventi per i data store di eventi che raccolgono eventi di gestione, eventi relativi ai dati ed eventi Insights. Queste dashboard sono gestite da CloudTrail Lake. Non puoi modificare, aggiungere o rimuovere i widget per queste dashboard, tuttavia, puoi salvare una dashboard gestita come dashboard personalizzata se desideri modificare i widget o impostare una pianificazione di aggiornamento.

> **Note**
>
> Puoi visualizzare solo i dashboard gestiti per gli archivi di dati sugli eventi presenti nel tuo account.

Per visualizzare un pannello di controllo gestito

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. Da Dashboard gestiti, scegli la dashboard che desideri visualizzare. Per ulteriori informazioni, consulta Dashboard gestiti disponibili.

   > **Note**
   >
   > Il menu a discesa mostra solo gli archivi di dati sugli eventi pertinenti per la dashboard selezionata. Ad esempio, se scegli dashboard incentrati sugli eventi relativi ai dati, come gli eventi relativi ai dati di S3, il menu a discesa mostrerà solo gli archivi di dati degli eventi configurati per raccogliere eventi di dati.

5. Scegli l'archivio dati degli eventi per la dashboard. CloudTrail eseguirà interrogazioni su questa dashboard quando la dashboard viene aggiornata.
6. Per visualizzare la query per un widget, scegli Visualizza e modifica la query nella parte inferiore del widget.
7. Puoi decidere di filtrare i dati del pannello di controllo in base a un Intervallo assoluto o un Intervallo relativo. Scegli Intervallo assoluto per selezionare un intervallo di data e ora specifico. Scegli Intervallo relativo per selezionare un intervallo di tempo predefinito o un intervallo personalizzato. Per impostazione predefinita, il pannello di controllo mostra i dati di eventi delle ultime 24 ore.

> **Note**
>
> CloudTrail Le query sul lago comportano costi in base alla quantità di dati scansionati. Per controllare i costi, puoi filtrare in base a un intervallo di tempo più ristretto. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

8. Scegli l'icona di aggiornamento per popolare la grafica dei widget della dashboard. Ogni widget indica lo stato dell'aggiornamento.

Salva una dashboard gestita come dashboard personalizzata

Non è possibile modificare una dashboard gestita, ma è possibile salvarne una copia come dashboard personalizzata. Ciò consente di impostare una pianificazione di aggiornamento per la dashboard e modificare i widget.

Per salvare una dashboard gestita come dashboard personalizzata

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. Scegli la dashboard gestita di cui desideri creare una copia.
5. Scegli Salva come nuova dashboard.
6. Fornisci un nome per identificare la dashboard.
7. (Facoltativo) Nella sezione Tag, puoi aggiungere fino a 50 coppie di chiavi di tag per aiutarti a identificare e ordinare i dashboard. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.
8. Per Autorizzazioni, scegli gli archivi di dati degli eventi a cui desideri applicare le autorizzazioni. Poiché CloudTrail esegue query per compilare i dati per i widget in una dashboard, CloudTrail richiede le autorizzazioni per eseguire query sul data store degli eventi associato ai widget della dashboard. Per ogni event data store selezionato in questo passaggio, CloudTrail allega una policy basata sulle risorse all'event data store che consente di eseguire query. CloudTrail È possibile deselezionare un Event Data Store se non si desidera consentire le autorizzazioni.
9. Seleziona Crea pannello di controllo.

Dopo aver creato la dashboard personalizzata, puoi aggiungere widget, rimuovere widget e impostare una pianificazione di aggiornamento per la dashboard.

Dashboard gestiti disponibili

La sezione fornisce informazioni sui dashboard gestiti disponibili e fornisce informazioni sui widget presenti in ogni dashboard.

Dashboard gestiti disponibili:

- Dashboard di monitoraggio della sicurezza
- Dashboard delle attività IAM
- Dashboard delle attività degli utenti
- Dashboard degli eventi arricchito
- Dashboard di analisi degli errori
- EC2 dashboard delle attività
- Dashboard delle attività di Organizations
- Dashboard delle modifiche alle risorse
- Pannello di panoramica degli eventi relativi ai dati
- Dashboard degli eventi dei dati Lambda
- Dashboard degli eventi dei dati DynamoDB
- Dashboard degli eventi relativi ai dati S3
- Dashboard degli eventi Insights
- Dashboard degli eventi di gestione
- Dashboard panoramica

Dashboard di monitoraggio della sicurezza

Questa dashboard offre una visualizzazione centralizzata dei widget critici incentrati sulla sicurezza, ad esempio gli eventi di accesso negato, i tentativi di accesso falliti alla console e gli indirizzi IP associati, i tentativi di accesso alla console dell'utente root, le azioni distruttive, l'accesso tra account e altri widget critici incentrati sulla sicurezza. Fornisce un rilevamento e una risposta rapidi agli incidenti per migliorare il livello di sicurezza generale.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

Principali eventi ad accesso negato

Tiene traccia degli eventi di accesso negato che si verificano più frequentemente, raggruppati per API.

ConsoleLogin Tentativi falliti

Monitora l'andamento dei tentativi falliti di accesso alla console nel corso del tempo, con interruzioni tra chiamanti autenticati tramite MFA e chiamanti non autenticati tramite MFA.

ConsoleLogin Tentativi falliti per indirizzo IP

Tiene traccia degli indirizzi IP associati ai tentativi di accesso falliti alla console e visualizza gli indirizzi IP più pericolosi in base al numero di accessi non riusciti.

Tentativi degli utenti ConsoleLogin root

Tiene traccia della frequenza dei tentativi di accesso alla console effettuati dagli utenti root nel tempo.

Azioni distruttive

Tiene traccia della frequenza delle operazioni di eliminazione nel tempo.

Accesso principale tra più account

Tiene traccia delle principali attività tra account in base all'ID dell'account chiamante e all'azione.

Utenti che hanno disabilitato l'MFA

Tiene traccia degli utenti più recenti che hanno disabilitato l'MFA.

Recenti EC2 SecurityGroup e modifiche NetworkAcl

Tiene traccia degli ultimi aggiornamenti EC2 SecurityGroup e NetworkAcl delle modifiche.

EC2 SecurityGroup Modifiche recenti che consentono l'accesso pubblico

Tiene traccia dei gruppi EC2 di sicurezza più recenti che dispongono di regole che consentono l'accesso pubblico (0.0.0.0/0).

Potenziali azioni di disabilitazione CloudTrail

Tiene traccia delle azioni recenti che rischiano di interrompere la registrazione. CloudTrail

Dashboard delle attività IAM

Questa dashboard offre visibilità sull'IAM di uso comune APIs, sugli errori API, sulle modifiche alle entità IAM e sugli indirizzi IP dei principali chiamanti, consentendo l'identificazione di azioni IAM non intenzionali e problemi di conformità.

Questa dashboard è disponibile per gli archivi di dati di eventi che raccolgono eventi di gestione e include i seguenti widget:

I migliori IAM APIs

Tiene traccia dell'IAM utilizzato più di frequente APIs.

I principali chiamanti IAM

Tiene traccia dei chiamanti dell'API IAM più frequenti.

Tendenza tra successo e fallimento di IAM

Monitora l'andamento delle chiamate API IAM riuscite e non riuscite nel tempo.

I principali errori dell'API IAM

Tiene traccia degli errori più frequenti nelle chiamate a IAM APIs.

I migliori AccessDenied IAM APIs

Tiene traccia delle chiamate API IAM più frequenti che non sono riuscite con errori di accesso negato.

I principali indirizzi IP delle chiamate IAM

Tiene traccia dei principali indirizzi IP di origine da cui sono state effettuate le chiamate API IAM.

Modifiche recenti alla politica IAM

Tiene traccia delle modifiche più recenti alle policy IAM, classificate in base alla specifica operazione dell'API IAM che ha facilitato la modifica, alla risorsa IAM (utente, ruolo o gruppo) associata alla modifica della policy e al nome della policy o ARN utilizzato.

Modifiche recenti degli utenti IAM

Tiene traccia delle modifiche più recenti degli utenti IAM, classificate in base alla specifica API IAM che facilita la gestione degli utenti, all'utente IAM interessato dalla modifica e all'ora dell'evento.

Principali ruoli IAM assunti

Tiene traccia dei ruoli IAM assunti più frequentemente.

Dashboard delle attività degli utenti

Questa dashboard offre visibilità sulle tendenze delle attività degli utenti, approfondimenti su aree chiave come gli utenti più attivi, i modelli di traffico degli utenti, gli utenti con errori di accesso negato, le operazioni recenti degli utenti, gli utenti che hanno eseguito attività distruttive e le modifiche alle politiche IAM, nonché le azioni degli utenti con privilegi. Aiuta a rilevare le azioni involontarie degli utenti e i rischi per la sicurezza.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

Tendenze delle attività degli utenti per ARN dell'utente

Tiene traccia dell'andamento dell'attività dell'utente nel tempo in base all'ARN dell'utente.

Tendenze delle attività degli utenti per API

Tiene traccia dell'andamento dell'attività degli utenti nel tempo tramite API.

Attività utente più recente

Tiene traccia delle azioni più recenti dell'utente.

Principali utenti con errori

Tiene traccia degli utenti con il maggior numero di errori.

Principali utenti con AccessDenied errori

Tiene traccia degli utenti con il maggior numero di AccessDenied errori.

Principali utenti che compiono azioni distruttive

Tiene traccia degli utenti che compiono il maggior numero di azioni distruttive.

Principali utenti che modificano le policy IAM

Tiene traccia degli utenti IAM che apportano frequentemente modifiche alle policy IAM.

Principali azioni eseguite da potenziali utenti con privilegi IAM

Tiene traccia delle azioni più frequenti degli utenti IAM con privilegi elevati, come gli amministratori.

Dashboard degli eventi arricchito

Questa dashboard arricchita degli eventi fornisce informazioni sulle tendenze relative alle risorse taggate, alle attività principali e ai criteri di condizione AWS globali. Queste informazioni ti aiutano ad analizzare le distribuzioni più frequenti di risorse e tag principali, nonché le chiavi di condizione globali utilizzate di frequente nelle sessioni di ruolo, nelle richieste e nei principali nel contesto delle richieste.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

Eventi arricchiti nel tempo

Tiene traccia del numero di eventi arricchiti nel tempo.

Le coppie chiave-valore dei tag di risorsa più frequenti

Visualizza le coppie chiave-valore dei tag di risorsa utilizzate più di frequente negli eventi arricchiti.

Le coppie chiave-valore dei tag di risorsa più frequenti con le risorse e gli utenti associati

Visualizza le coppie chiave-valore dei tag di risorsa utilizzate più di frequente, mostrando quali risorse utilizzano questi tag e quali utenti sono associati ad essi.

Le coppie chiave-valore dei tag principali più frequenti

Visualizza le coppie chiave-valore dei tag principali utilizzate più di frequente negli eventi arricchiti.

Le azioni di accesso negato più frequenti, raggruppate per coppie chiave-valore dei tag principali.

Visualizza le azioni di accesso negato più frequenti raggruppate per coppie chiave-valore dei tag principali in tutti gli eventi arricchiti.

Le proprietà principali più frequenti nelle chiavi di condizione globali IAM

Visualizza le chiavi di condizione globali IAM utilizzate più di frequente per le proprietà principali, mostrandone le coppie chiave-valore e i conteggi in tutti gli eventi.

Le proprietà di richiesta più frequenti nelle chiavi di condizione globali IAM

Visualizza le chiavi di condizione globali IAM utilizzate più di frequente per le proprietà della richiesta, mostrandone le coppie chiave-valore e i conteggi in tutti gli eventi.

Le proprietà delle sessioni di ruolo più frequenti nelle chiavi di condizione globali IAM

Visualizza le chiavi di condizione globali IAM utilizzate più di frequente per le proprietà delle sessioni di ruolo, mostrandone le coppie chiave-valore e i conteggi in tutti gli eventi.

Dashboard di analisi degli errori

Questa dashboard fornisce informazioni complete sulle tendenze degli errori tra servizi, utenti APIs, codici di errore e throttled APIs. La visibilità consente l'identificazione e la risoluzione tempestive di potenziali problemi di disponibilità per prestazioni ottimali del sistema.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

Conteggio degli errori per servizio

Tiene traccia del conteggio degli errori delle attività per servizio.

Conteggio degli errori per API

Tiene traccia del conteggio degli errori delle attività per API.

Principali errori in base al codice di errore

Tiene traccia degli errori più frequenti in base al codice di errore.

Principali errori per messaggio di errore

Tiene traccia degli errori più frequenti tramite messaggio di errore.

Principali AccessDenied errori per API

Tiene traccia degli APIs errori di accesso negato segnalati più frequentemente.

Principali errori limitati per API

Tiene traccia degli APIs errori limitati segnalati più frequentemente.

Principali utenti con errori

Tiene traccia degli utenti con gli errori segnalati più frequentemente.

EC2 dashboard delle attività

Questa dashboard offre una visibilità completa sulle attività di EC2 gestione, come le tendenze delle API, gli errori di accesso, i principali lanciatori di istanze, le modifiche alla sicurezza e le modifiche alla rete. Gli approfondimenti aiutano a identificare i rischi per la sicurezza e i problemi operativi.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

EC2 panoramica delle attività di gestione delle istanze

Monitora una panoramica delle attività di gestione delle EC2 istanze in un periodo di tempo specificato, evidenziando le operazioni chiave come avvii, arresti e terminazioni.

EC2 Tendenze di successo e fallimento delle API

Monitora l'andamento delle chiamate EC2 API riuscite e non riuscite nel tempo.

I principali EC2 errori

Tiene traccia dei codici di errore più frequenti che si verificano durante le chiamate EC2 API.

I migliori EC2 AccessDenied eventi

Tracce EC2 APIs con il maggior numero di errori di accesso negato.

Principali utenti che EC2 lanciano istanze

Tiene traccia degli utenti più attivi nel lancio di nuove istanze. EC2

Recenti EC2 SecurityGroup e modifiche NetworkInterface

Tiene traccia delle modifiche più recenti al gruppo EC2 di sicurezza e all'interfaccia di rete.

Gestione VPC recente e modifiche alla tabella di routing

Tiene traccia delle attività di gestione dei VPC più recenti e delle modifiche alla tabella di routing.

EC2 Azioni recenti dell'utente root

Tiene traccia delle EC2 azioni più recenti eseguite dagli utenti root con autorizzazioni altamente privilegiate.

Dashboard delle attività di Organizations

Progettata per gli archivi di dati sugli eventi organizzativi, questa dashboard offre visibilità sulle attività e sulle tendenze organizzative, comprese informazioni sui membri attivi, sulla gestione degli account, sui modelli di accesso, sulle modifiche alle politiche e sui principali servizi e APIs utilizzati.

Questa dashboard è disponibile per gli archivi dati degli eventi organizzativi e include i seguenti widget:

Tendenza delle attività nell'organizzazione

Tiene traccia dell'andamento generale delle attività AWS Organizations nell'intera organizzazione nel tempo, fornendo visibilità nei periodi di alti o bassi livelli di attività.

Riepilogo della gestione degli account dei membri

Tiene traccia della distribuzione delle attività di gestione degli account dei membri all'interno dell'organizzazione, classificate in base ai conteggi di ciascun tipo di attività.

I servizi più utilizzati in tutta l'organizzazione

Tiene traccia di quelli Servizi AWS che sono stati maggiormente utilizzati in tutta l'organizzazione.

Account più attivi per servizio

Tiene traccia degli account più attivi utilizzando un account all' Servizio AWS interno dell'organizzazione.

I più utilizzati APIs in tutta l'organizzazione

Evidenzia quelli AWS APIs che sono stati richiamati più frequentemente in tutta l'organizzazione.

Account dei membri più attivi

Tiene traccia degli account dei membri dell'organizzazione che hanno registrato il maggior numero di attività.

Tendenza degli errori di accesso negato in tutta l'organizzazione

Tiene traccia dello schema degli errori di accesso negato che si verificano all'interno dell'organizzazione nel tempo.

Account con la maggior parte degli errori di accesso negato

Tiene traccia degli account all'interno dell'organizzazione che hanno riscontrato il maggior numero di errori di accesso negato.

Modifiche recenti alla politica di controllo dei servizi

Tiene traccia delle modifiche più recenti apportate alle politiche di controllo del servizio (SCPs) all'interno dell'organizzazione.

Dashboard delle modifiche alle risorse

Questa dashboard offre una visione completa delle attività di gestione delle risorse e monitora le tendenze in termini di approvvigionamento, eliminazione e modifiche tra i servizi. Evidenzia le modifiche critiche, comprese quelle apportate manualmente e a policy come il bucket S3 e l'accesso KMS. AWS CloudFormation

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di gestione e include i seguenti widget:

Tendenze di creazione ed eliminazione delle risorse

Tiene traccia della creazione e dell'eliminazione di risorse all'interno dell'account nel tempo.

Principali utenti che si occupano della creazione di risorse

Tiene traccia degli utenti che creano nuove risorse più attivamente.

APIs Utilizzato principalmente per la creazione di risorse

Tiene traccia delle risorse APIs utilizzate più di frequente per creare nuove risorse all'interno dell'account.

Principalmente APIs utilizzato per l'eliminazione delle risorse

Tiene traccia delle risorse APIs utilizzate più di frequente per eliminare le risorse all'interno dell'account.

Le risorse più recenti create all'esterno CloudFormation

Tiene traccia delle nuove risorse create al di fuori della CloudFormation governance, evidenziando le modifiche non gestite tramite CloudFormation modelli.

Le modifiche più recenti alle risorse apportate tramite console

Tiene traccia delle modifiche più recenti apportate alle risorse tramite AWS Management Console.

Le modifiche più recenti all'accesso ai bucket S3

Tiene traccia delle modifiche più recenti all'accesso ai bucket S3.

Le modifiche più recenti all'accesso tramite chiave KMS

Tiene traccia delle modifiche più recenti alle politiche chiave del KMS.

Pannello di panoramica degli eventi relativi ai dati

Questa dashboard offre una visualizzazione centralizzata degli eventi relativi ai dati nell'Event Data Store, tra cui le tendenze complessive delle attività, i servizi principali APIs, le regioni, il piano dati limitato e i principali APIs utenti del piano dati. Questa dashboard consente di monitorare l'attività dell'API Data Plane per il controllo e la risoluzione dei problemi.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di dati e include i seguenti widget:

Tendenza complessiva degli eventi relativi ai dati

Tiene traccia dell'andamento degli eventi complessivi relativi ai dati che si verificano all'interno dell'account nel tempo.

I migliori servizi che generano eventi relativi ai dati

Tiene traccia dei servizi che generano il maggior volume di attività di dati all'interno dell'account.

Principali eventi APIs di generazione di dati

Tiene traccia dell'attività APIs generata dal maggior volume di dati all'interno dell'account.

Principali regioni che generano eventi relativi ai dati

Tiene traccia delle regioni che generano il maggior volume di attività relative ai dati all'interno dell'account.

Il piano dati con la massima limitazione APIs

Tiene traccia del piano dati APIs che subisce frequenti limitazioni all'interno dell'account.

Principali utenti del piano dati APIs

Tiene traccia degli utenti principali che utilizzano APIs maggiormente il piano dati in tutto l'account.

Dashboard degli eventi dei dati Lambda

Questa dashboard offre visibilità sull'attività dell'API del piano dati Lambda, inclusi gli utenti principali, le funzioni richiamate di frequente e gli errori API più comuni. Queste informazioni consentono di controllare l'utilizzo di Lambda, rilevare anomalie e mitigare i rischi operativi o di sicurezza.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi dati Lambda e include i seguenti widget:

Attività dell'API del piano dati Lambda

Tiene traccia dell'andamento dell'attività dell'API del piano dati Lambda all'interno dell'account nel tempo.

Tendenza tra successo e fallimento delle chiamate Lambda

Monitora l'andamento delle chiamate Lambda riuscite e non riuscite nel tempo.

Principali utenti delle chiamate Lambda

Tiene traccia degli utenti che effettuano il maggior numero di chiamate delle funzioni Lambda nell'account.

Principali funzioni Lambda richiamate

Tiene traccia delle funzioni Lambda richiamate più frequentemente all'interno dell'account.

I 10 principali errori dell'API Lambda Invoke

Tiene traccia dei 10 errori principali riscontrati durante le chiamate API Lambda Invoke.

Gli utenti più limitati delle chiamate Lambda

Tiene traccia degli utenti che sperimentano il maggior numero di eventi di limitazione per le chiamate Lambda.

Dashboard degli eventi dei dati DynamoDB

Questa dashboard offre visibilità sull'attività dell'API del piano dati di DynamoDB, incluse le tendenze di utilizzo, i APIs top e i modelli di limitazione che coinvolgono utenti e tabelle. Queste informazioni consentono di controllare l'utilizzo di DynamoDB, rilevare anomalie e mitigare i rischi operativi o di sicurezza.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di dati DynamoDB e include i seguenti widget:

Attività dei dati dell'account DynamoDB

Tiene traccia dell'andamento degli eventi relativi ai dati di DynamoDB che si verificano all'interno dell'account nel tempo.

Tendenza tra successo e fallimento del APIs piano dati DynamoDB

Monitora l'andamento delle chiamate API del piano dati DynamoDB riuscite e non riuscite nel tempo.

I 10 migliori piani dati DynamoDB APIs

Elenca le 10 principali chiamate API del piano dati DynamoDB.

Principali utenti del piano dati DynamoDB APIs

Tiene traccia degli utenti che effettuano il maggior numero di chiamate al APIs piano dati DynamoDB all'interno dell'account.

I 10 principali errori delle API del piano dati DynamoDB

Tiene traccia dei 10 errori principali nella chiamata al piano dati DynamoDB. APIs

Gli utenti più limitati del piano dati DynamoDB APIs

Tiene traccia degli utenti con limitazioni più frequenti quando chiamano il piano dati DynamoDB. APIs

Il piano dati DynamoDB con la massima limitazione APIs

Tiene traccia del APIs piano dati di DynamoDB che subisce frequenti rallentamenti all'interno dell'account.

Le migliori tabelle DynamoDB con limitazioni

Tiene traccia delle tabelle DynamoDB che presentano i più alti tassi di throttling all'interno dell'account.

Dashboard degli eventi relativi ai dati S3

Questa dashboard offre visibilità sull'attività dell'API del piano dati S3, comprese le tendenze di utilizzo, gli oggetti S3 più utilizzati, i principali utenti S3 e le principali azioni S3. Queste informazioni ti aiutano a controllare l'utilizzo di S3, rilevare anomalie e mitigare i rischi operativi o di sicurezza.

Questa dashboard è disponibile per i data store di eventi che raccolgono eventi di dati di Amazon S3 e include i seguenti widget:

Attività dell'account S3

Tiene traccia dell'attività dell'account S3.

Oggetti più accessibili

Elenca gli oggetti S3 più accessibili.

Principali utenti di S3

Tiene traccia dei principali utenti di S3.

Principali azioni S3

Tiene traccia delle azioni principali di S3.

Dashboard degli eventi Insights

Questa dashboard offre visibilità sulla suddivisione complessiva degli eventi di Insights per tipo, nonché sui principali utenti e servizi che generano questi tipi di eventi. Inoltre, mostra il conteggio giornaliero degli eventi di Insights e una visualizzazione storica di 30 giorni delle metriche di Insights.

> **Note**
>
> - Dopo aver abilitato CloudTrail Insights per la prima volta nell'archivio dati degli eventi di origine, possono essere necessari fino a 7 giorni per CloudTrail la distribuzione del primo evento Insights, se viene rilevata un'attività insolita.
> - Il pannello di controllo Eventi Insights mostra solo le informazioni sugli eventi Insights raccolti dalil datastore di eventi selezionato, che è determinato dalla configurazione delil datastore di eventi di origine. Ad esempio, se configuri il datastore di eventi di origine per abilitare gli eventi Insights su `ApiCallRateInsight` ma non su `ApiErrorRateInsight`, non vedrai le informazioni sugli eventi Insights su `ApiErrorRateInsight`.

Questa dashboard è disponibile per gli archivi di dati di eventi che raccolgono eventi Insights e include i seguenti widget:

Tipi di Insight

Tiene traccia degli eventi in base al tipo di Insights.

Approfondimenti per data

Tiene traccia degli eventi di Insights per data.

Frequenza delle chiamate API Insights per origine dell'evento

Monitora la frequenza delle chiamate API Insights in base all'origine dell'evento. Per visualizzare i dati di questo widget, il data store degli eventi di Insights deve essere configurato per raccogliere Insights sulla frequenza delle chiamate API.

Tasso di errore delle API Insights per origine dell'evento

Tiene traccia del tasso di errore delle API Insights in base all'origine dell'evento. Per visualizzare questo widget, il data store degli eventi di Insights deve essere configurato per raccogliere Insights sul tasso di errore dell'API.

Informazioni fornite dai migliori utenti

Elenca i principali utenti con richieste che generano eventi Insights.

Eventi Insights

Elenca gli eventi recenti di Insights.

Dashboard degli eventi di gestione

Questa dashboard evidenzia informazioni dettagliate sugli eventi di accesso negato, sulle azioni distruttive, sugli eventi di accesso alla console, sui principali errori per utente, sull'utilizzo della versione TLS e sulle chiamate TLS obsolete da parte dell'utente.

Questa dashboard è disponibile per gli archivi di dati sugli eventi che raccolgono eventi di gestione e include i seguenti widget:

Principali eventi ad accesso negato

Tiene traccia dei principali eventi che hanno provocato errori di accesso negato.

Principali errori per utente

Tiene traccia dei principali errori per utente.

Eventi di accesso alla console

Mostra gli eventi di accesso alla console.

Azioni distruttive

Tiene traccia delle azioni che hanno portato ad azioni distruttive.

Versione TLS

Mostra le versioni TLS.

Chiamate TLS obsolete da parte dell'utente

Tiene traccia delle chiamate che utilizzano versioni TLS obsolete per utente.

Dashboard panoramica

Questa dashboard evidenzia informazioni dettagliate sugli eventi di accesso negato, sulle azioni distruttive, sugli eventi di accesso alla console, sui principali errori per utente, sull'utilizzo della versione TLS e sulle chiamate TLS obsolete da parte dell'utente.

Questa dashboard è disponibile per gli archivi di dati sugli eventi che raccolgono eventi di gestione e include i seguenti widget:

Attività dell'account

Monitora l'attività di lettura e scrittura del tuo account.

Errori principali

Elenca gli errori più frequenti.

Regioni più attive

Mostra le più attive Regioni AWS.

I migliori servizi

Mostra i migliori servizi.

Gli eventi più limitati

Elenca gli eventi più limitati.

Utenti principali

Elenca gli utenti principali.

Abilita la dashboard Highlights con la CloudTrail console

Abilita la dashboard Highlights per visualizzare una at-a-glance panoramica dell' AWS attività raccolta dagli archivi di dati sugli eventi nel tuo account. La dashboard Highlights è gestita CloudTrail e include widget pertinenti al tuo account. I widget mostrati nella dashboard Highlights sono unici per ogni account. Questi widget potrebbero far emergere attività o anomalie rilevate. Ad esempio, la dashboard Highlights potrebbe includere il widget Total cross-account access, che mostra se c'è un aumento delle attività anomale tra account.

CloudTrail aggiorna la dashboard Highlights ogni 6 ore. La dashboard mostra i dati delle ultime 24 ore dall'ultimo aggiornamento.

> **Note**
>
> Puoi abilitare la dashboard Highlights solo per gli archivi di dati sugli eventi esistenti nel tuo account.
> Non puoi impostare una pianificazione di aggiornamento per la dashboard Highlights o aggiungere o rimuovere widget.

Per abilitare la dashboard Highlights

Utilizza la seguente procedura per abilitare la dashboard Highlights.

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Highlights.
4. Poiché l'esecuzione delle query comporta dei CloudTrail costi, ti CloudTrail chiede di esaminare le informazioni sui costi prima di attivare la dashboard Highlights. Per informazioni sui CloudTrail prezzi, consulta la sezione AWS CloudTrail Prezzi.

   Scegli Accetto e abilita Highlights per abilitare la dashboard Highlights.
5. Per Autorizzazioni, scegli gli archivi di dati degli eventi a cui desideri applicare le autorizzazioni. CloudTrail richiede le autorizzazioni per eseguire interrogazioni sui data store degli eventi e aggiornare la dashboard per tuo conto. Per fornire le autorizzazioni, CloudTrail associa una policy predefinita basata sulle risorse a ogni event data store selezionato in questo passaggio per consentire CloudTrail l'esecuzione di query sul data store degli eventi. CloudTrail allega una policy basata sulle risorse alla dashboard per consentire l'aggiornamento della dashboard ogni 6 ore. CloudTrail

   È possibile modificare la politica basata sulle risorse per un data store di eventi dalla relativa pagina dei dettagli. È possibile modificare la politica basata sulle risorse per una dashboard selezionando Modifica politica dal menu Azioni della dashboard.
6. Scegli Conferma.

Quando abiliti la dashboard Highlights, la protezione dalla terminazione viene abilitata automaticamente. La protezione dalla terminazione protegge un pannello di controllo

dall'eliminazione accidentale. Dovrai disabilitare la protezione dalla terminazione, se desideri disabilitare la dashboard.

Disattiva la dashboard Highlights con la console CloudTrail

Questa sezione descrive come disabilitare la dashboard Highlights. Poiché la protezione dalla terminazione è abilitata automaticamente per la dashboard Highlights, devi prima disabilitare la protezione dalla terminazione e poi disabilitare la dashboard Highlights.

Per disabilitare la dashboard Highlights

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Highlights.
4. Da Operazioni, scegli Modifica protezione della terminazione.
5. Scegli Disabilita.
6. Scegli Save (Salva).
7. Da Azioni, scegli Disabilita le evidenziazioni.

Crea una dashboard personalizzata con la CloudTrail console

Puoi creare dashboard personalizzate e aggiungere fino a 10 widget a ciascuna dashboard personalizzata. Puoi scegliere di aggiungere widget di esempio o creare nuovi widget da query SQL.

Dopo aver aggiunto i widget, puoi aggiornare manualmente la dashboard o impostare una pianificazione di aggiornamento.

Per creare un pannello di controllo personalizzato

1. Accedi AWS Management Console e apri la console all'indirizzo. CloudTrail https://console.aws.amazon.com/cloudtrail/
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. Scegli Crea la mia dashboard.
5. Fornisci un nome per identificare la dashboard.

6. Per Autorizzazioni, scegli gli archivi di dati degli eventi a cui desideri applicare le autorizzazioni. Poiché CloudTrail esegue query per compilare i dati per i widget in una dashboard, CloudTrail richiede le autorizzazioni per eseguire query sugli archivi di dati degli eventi associati ai widget della dashboard. Per ogni data store di eventi selezionato in questo passaggio, CloudTrail allega una policy basata sulle risorse all'event data store che consente di eseguire query sul data store degli eventi CloudTrail per questa dashboard.
7. (Facoltativo) Nella sezione Tag, puoi aggiungere fino a 50 coppie di chiavi di tag per aiutarti a identificare e ordinare i dashboard. Per ulteriori informazioni su come utilizzare i tag in AWS, consulta Tagging AWS resources nella Tagging Resources User AWS Guide.
8. Seleziona Crea pannello di controllo.

   Successivamente, puoi aggiungere widget e impostare una pianificazione di aggiornamento.

Argomenti

- Aggiungi un widget di esempio con la console CloudTrail
- Crea un nuovo widget da una query SQL con la CloudTrail console
- Rimuovi un widget da una dashboard con la CloudTrail console

Aggiungi un widget di esempio con la console CloudTrail

Questa sezione descrive come aggiungere un widget di esempio alla dashboard. Puoi aggiungere un massimo di 10 widget a una dashboard personalizzata.

> **Note**
>
> I widget di esempio sono limitati a un singolo archivio di dati di eventi presente nel tuo account. Per eseguire query su più archivi di dati di eventi presenti nel tuo account, crea un nuovo widget.

Per aggiungere un widget di esempio a una dashboard

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.

4. In Dashboard personalizzati, scegli la dashboard a cui desideri aggiungere un widget.
5. Da Azioni, scegli Modifica dashboard.
6. Da Azioni, scegli Aggiungi widget di esempio.
7. Scegli il data store degli eventi su cui eseguire la query. Puoi scegliere solo i data store di eventi presenti nel tuo account.
8. Scegli il widget di esempio che desideri aggiungere. Per impostazione predefinita, vengono visualizzati tutti i widget di esempio. Puoi filtrare in base al tipo di widget (ad esempio, i widget IAM).
9. Scegli Visualizza interrogazione per visualizzare la query per il widget selezionato.
10. Scegli Aggiungi alla dashboard per aggiungere il widget alla dashboard.
11. Scegli Salva per salvare la dashboard.

Crea un nuovo widget da una query SQL con la CloudTrail console

Questa sezione descrive come creare un nuovo widget scrivendo o incollando una query SQL e scegliendo un tipo di grafico. Puoi aggiungere un massimo di 10 widget a una dashboard personalizzata.

Per creare un nuovo widget da una query SQL

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. In Dashboard personalizzati, scegli la dashboard per cui desideri creare un widget.
5. Da Azioni, scegli Modifica dashboard.
6. Da Azioni, scegli Crea nuovo widget.
7. Scegli il data store degli eventi su cui eseguire la query. Puoi eseguire query su più archivi dati di eventi purché gli archivi dati degli eventi esistano nel tuo account.
8. Scrivi o copia la query SQL.

   Puoi anche fornire un prompt in linguaggio naturale in inglese e scegliere Genera query per generare una query SQL dal tuo prompt. Per ulteriori informazioni, consulta Crea query su CloudTrail Lake da istruzioni in linguaggio naturale.

9. Scegliete Esegui per eseguire la query e visualizzare in anteprima i risultati della query.

> **Note**
>
> Quando esegui le query, ti vengono addebitati dei costi in base alla quantità di dati ottimizzati e compressi scansionati. Per aiutare a controllare i costi, si consiglia di limitare le query aggiungendo data e ora di inizio e fine alle query. `eventTime`

10. Scegli la scheda Visualizer per selezionare il tipo di grafico per il widget. Puoi scegliere tra questi tipi di grafico: tabella, grafico a barre, grafico a linee e grafico a torta.
11. Scegli Aggiungi alla dashboard per aggiungere il widget alla dashboard.
12. Scegli Salva per salvare la dashboard.

Rimuovi un widget da una dashboard con la CloudTrail console

Questa sezione descrive come rimuovere un widget da una dashboard personalizzata.

Per rimuovere un widget da una dashboard

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. In Dashboard personalizzati, scegli la dashboard per la quale desideri rimuovere un widget.
5. Da Azioni, scegli Modifica dashboard.
6. Sul widget che desideri rimuovere, scegli l'icona di rimozione ( ), quindi scegli Rimuovi.
7. Scegli Salva per salvare la dashboard.

Imposta una pianificazione di aggiornamento per una dashboard personalizzata con la console CloudTrail

Questa sezione descrive come impostare una pianificazione di aggiornamento della dashboard. Puoi impostare una pianificazione di aggiornamento per consentire a CloudTrail Lake di aggiornare una dashboard ogni 1 ora, 6 ore, 12 ore o 24 ore (1 giorno).

Quando imposti una pianificazione di aggiornamento utilizzando la CloudTrail console, CloudTrail allega alla dashboard una politica basata sulle risorse che consente di aggiornare la dashboard CloudTrail per tuo conto.

Per impostare una pianificazione di aggiornamento

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. In Dashboard personalizzati, scegli la dashboard per cui desideri impostare una pianificazione di aggiornamento.
5. Scegli la frequenza di aggiornamento dall'elenco a discesa.
6. Per creare una pianificazione di aggiornamento, CloudTrail allega alla dashboard una politica basata sulle risorse per consentire l'aggiornamento della dashboard per tuo conto CloudTrail . Espandi la politica delle risorse della dashboard per visualizzare la politica basata sulle risorse da allegare alla dashboard. CloudTrail
7. Poiché l'esecuzione delle query comporta dei costi, ti CloudTrail chiede di confermare che desideri eseguire le query con la CloudTrail frequenza pianificata. Scegli Conferma per impostare una pianificazione di aggiornamento.

Disattiva la pianificazione dell'aggiornamento per una dashboard personalizzata con la console CloudTrail

Puoi disabilitare la pianificazione degli aggiornamenti se non desideri più CloudTrail aggiornare automaticamente la dashboard e desideri invece aggiornare manualmente la dashboard.

Per disabilitare una pianificazione di aggiornamento

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra, in Lake, seleziona Pannello di controllo.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. In Dashboard personalizzati, scegli la dashboard per cui desideri disabilitare una pianificazione di aggiornamento.
5. Scegli Disabilita la pianificazione degli aggiornamenti dall'elenco a discesa.

Modifica la protezione dalla terminazione con la console CloudTrail

La protezione dalla terminazione impedisce l'eliminazione accidentale di un pannello di controllo. Se desideri eliminare una dashboard personalizzata o disabilitare la dashboard Highlights, devi disabilitare la protezione dalla terminazione.

Per disattivare la protezione della terminazione

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, sotto Lake, scegli Dashboard.
3. Scegli la dashboard per cui desideri disabilitare la protezione dalla terminazione.
4. Da Operazioni, scegli Modifica protezione della terminazione.
5. Scegli Disabilita.
6. Scegli Save (Salva).

Per attivare la protezione della terminazione

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, sotto Lake, scegli Dashboard.
3. Scegli la dashboard per cui desideri abilitare la protezione dalla terminazione.
4. Da Operazioni, scegli Modifica protezione della terminazione.

5. Per attivare la protezione della terminazione, scegli Abilitata.
6. Scegli Save (Salva).

Elimina una dashboard personalizzata con la console CloudTrail

Questa sezione descrive come eliminare un pannello di controllo utilizzando CloudTrail.

> **Note**
>
> Non è possibile eliminare un Event Data Store se la protezione dalla terminazione è abilitata.

Eliminazione di un pannello di controllo

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, sotto Lake, scegli Dashboard.
3. Scegli la scheda Dashboard gestite e personalizzate.
4. Scegli la dashboard personalizzata che desideri eliminare.
5. In Operazioni, seleziona Elimina.
6. Scegli Elimina per confermare che desideri eliminare la dashboard.

Crea, aggiorna e gestisci i dashboard con AWS CLI

Questa sezione descrive i AWS CLI comandi che puoi utilizzare per creare, aggiornare e gestire le dashboard di CloudTrail Lake.

Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro `--region` con il comando.

Comandi disponibili per i dashboard

I comandi per la creazione e l'aggiornamento delle dashboard in CloudTrail Lake includono:

- `create-dashboard`per creare una dashboard personalizzata o abilitare la dashboard Highlights.

- `update-dashboard`per aggiornare una dashboard personalizzata o la dashboard Highlights.
- `delete-dashboard`per eliminare una dashboard personalizzata o la dashboard Highlights.
- `get-dashboard`restituisce informazioni sulla dashboard specificata.
- `list-dashboards`elenca tutte le dashboard per il tuo Account AWS o per il filtro specificato.
- `start-dashboard-refresh`avvia un aggiornamento della dashboard.
- `get-resource-policy`ottiene la politica basata sulle risorse allegata alla dashboard.
- `put-resource-policy`allega una policy basata sulle risorse a una dashboard per consentire l'aggiornamento asincrono della dashboard CloudTrail per conto dell'utente. È inoltre possibile allegare una policy basata sulle risorse a un data store di eventi per consentire l'esecuzione di interrogazioni sul data store degli eventi CloudTrail per compilare i dati per i widget del dashboard.
- `delete-resource-policy`rimuove la politica basata sulle risorse allegata a un dashboard.
- `add-tags`aggiunge tag per identificare la dashboard.
- `remove-tags`rimuove i tag da una dashboard.
- `list-tags`elenca i tag per una dashboard.

Per un elenco dei comandi disponibili per i data store di eventi CloudTrail Lake, vediComandi disponibili per gli archivi dati degli eventi.

Per un elenco dei comandi disponibili per le query CloudTrail Lake, consultaComandi disponibili per le query su CloudTrail Lake.

Per un elenco dei comandi disponibili per le integrazioni di CloudTrail Lake, consulta. Comandi disponibili per le integrazioni con CloudTrail Lake

Argomenti:

- Crea una dashboard con il AWS CLI
- Gestisci i pannelli di controllo con AWS CLI
- Eliminare un pannello di controllo con il AWS CLI

Crea una dashboard con il AWS CLI

Questa sezione descrive come utilizzare il `create-dashboard` comando per creare una dashboard personalizzata o la dashboard Highlights.

Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro `--region` con il comando.

CloudTrail esegue query per popolare i widget della dashboard durante un aggiornamento manuale o pianificato. CloudTrail è necessario disporre delle autorizzazioni per eseguire l'`StartQuery`operazione su ogni archivio dati di eventi associato a un widget del dashboard. Per fornire le autorizzazioni, esegui il `put-resource-policy` comando per allegare una policy basata sulle risorse a ciascun event data store oppure modifica la policy dell'Event Data Store sulla console. CloudTrail Per un esempio di policy, consulta Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard.

Per impostare una pianificazione di aggiornamento, è CloudTrail necessario disporre delle autorizzazioni necessarie per eseguire l'`StartDashboardRefresh`operazione di aggiornamento della dashboard per conto dell'utente. Per fornire le autorizzazioni, esegui l'`put-resource-policy`operazione per allegare una politica basata sulle risorse alla dashboard o modifica la politica della dashboard sulla console. CloudTrail Per un esempio di policy, consulta Esempio di policy basata sulle risorse per un pannello di controllo.

Esempi:

- Crea una dashboard personalizzata con AWS CLI
- Abilita il pannello di controllo Highlights con AWS CLI
- Visualizza le proprietà dei widget

Crea una dashboard personalizzata con AWS CLI

La procedura seguente mostra come creare un dashboard personalizzato, allegare le politiche basate sulle risorse richieste agli archivi di dati degli eventi e al dashboard e aggiornare il dashboard per impostare e abilitare una pianificazione di aggiornamento.

1. Esegui il comando per creare un pannello `create-dashboard` di controllo.

   Quando crei una dashboard personalizzata, puoi inserire un array con un massimo di 10 widget. Un widget fornisce una rappresentazione grafica dei risultati di una query. Ogni widget è composto da `ViewPropertiesQueryStatement`, `eQueryParameters`.

   - `ViewProperties`: specifica le proprietà per il tipo di visualizzazione. Per ulteriori informazioni, consulta Visualizza le proprietà dei widget.

- `QueryStatement`— La query CloudTrail viene eseguita quando il dashboard viene aggiornato. È possibile eseguire query su più archivi dati di eventi purché gli archivi dati degli eventi esistano nel proprio account.
- `QueryParameters`— I seguenti `QueryParameters` valori sono supportati per i dashboard personalizzati:`$Period$`,`$StartTime$`, e`$EndTime$`. Per utilizzare, `QueryParameters` posiziona `?` a nel `QueryStatement` punto in cui desideri sostituire il parametro. CloudTrail inserirà i parametri quando viene eseguita la query.

L'esempio seguente crea una dashboard con quattro widget, uno per ogni tipo di visualizzazione.

> **Note**
>
> In questo esempio, `?` è racchiuso tra virgolette singole perché viene utilizzato con`eventTime`. A seconda del sistema operativo in uso, potrebbe essere necessario racchiudere le virgolette singole tra virgolette di escape. Per ulteriori informazioni, vedere Utilizzo di virgolette e letterali con stringhe in. AWS CLI

```
aws cloudtrail create-dashboard --name AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
```

```
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT
100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "AccountActivity",
        "View": "LineChart",
        "YAxisColumn": "eventCount",
        "XAxisColumn": "eventDate",
        "FilterColumn": "readOnly"
      },
      "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate,
IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly
ORDER BY DATE_TRUNC('?', eventTime), readOnly",
      "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$",
"$Period$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Horizontal"
      },
      "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
  ]'
```

2. Esegui il `put-resource-policy` comando per allegare una politica basata sulle risorse a ogni archivio di dati di eventi incluso in un widget. `QueryStatement` Puoi anche aggiornare la politica basata sulle risorse di un Event Data Store sulla console. CloudTrail Per un esempio di policy, consulta Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard.

   L'esempio seguente allega una policy basata sulle risorse a un data store di eventi. Sostituiscilo *`account-id`* con l'ID del tuo account, *`eds-arn`* con l'ARN dell'archivio dati degli eventi per il quale CloudTrail verranno eseguite le query e con *`dashboard-arn`* l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" },
 "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

3. Esegui il `put-resource-policy` comando per allegare una politica basata sulle risorse alla dashboard. Per un esempio di policy, consulta Esempio di policy basata sulle risorse per un pannello di controllo.

   L'esempio seguente allega una policy basata sulle risorse a un pannello di controllo. Sostituiscilo *`account-id`* con l'ID del tuo account e *`dashboard-arn`* con l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid":
 "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. Esegui il `update-dashboard` comando per impostare e abilitare una pianificazione di aggiornamento configurando il parametro. `--refresh-schedule`

   `--refresh-schedule`È costituito dai seguenti parametri opzionali:

   - `Frequency`— La `Unit` e `Value` per la pianificazione.

     Per i dashboard personalizzati, l'unità può essere `HOURS` o`DAYS`.

     Per i dashboard personalizzati, i seguenti valori sono validi quando l'unità è`HOURS`:1,,, 6 12 24

Per i dashboard personalizzati, l'unico valore valido quando l'unità è è`DAYS`. 1

- `Status`— Speciifica se la pianificazione dell'aggiornamento è abilitata. Imposta il valore `ENABLED` per abilitare la pianificazione dell'aggiornamento o `DISABLED` per disattivarla.
- `TimeOfDay` — L'ora del giorno in UTC in cui eseguire la pianificazione; per ora si fa riferimento solo ai minuti; l'impostazione predefinita è 00:00.

L'esempio seguente imposta una pianificazione di aggiornamento ogni sei ore e abilita la pianificazione.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

Abilita il pannello di controllo Highlights con AWS CLI

La procedura seguente mostra come creare la dashboard Highlights, allegare le politiche basate sulle risorse richieste ai data store degli eventi e alla dashboard e aggiornare la dashboard per impostare e abilitare la pianificazione degli aggiornamenti.

1. Esegui il `create-dashboard` comando per creare la dashboard Highlights. Per creare questa dashboard, `--name` deve essere`AWSCloudTrail-Highlights`.

   ```
   aws cloudtrail create-dashboard --name AWSCloudTrail-Highlights
   ```

2. Per ogni archivio dati di eventi nel tuo account, esegui il `put-resource-policy` comando per allegare una politica basata sulle risorse all'archivio dati degli eventi. Puoi anche aggiornare la politica basata sulle risorse di un Event Data Store sulla console. CloudTrail Per un esempio di policy, consulta Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard.

   L'esempio seguente allega una policy basata sulle risorse a un data store di eventi. Sostituisci *`account-id`* con l'ID del tuo account, *`eds-arn`* con l'ARN dell'archivio dati degli eventi e *`dashboard-arn`* con l'ARN della dashboard.

   ```
   aws cloudtrail put-resource-policy \
   --resource-arn eds-arn \
   --resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
    "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" },
   ```

```
 "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

3. Esegui il `put-resource-policy` comando per allegare una politica basata sulle risorse alla dashboard. Per un esempio di policy, consulta Esempio di policy basata sulle risorse per un pannello di controllo.

   L'esempio seguente allega una policy basata sulle risorse a un pannello di controllo. Sostituiscilo *`account-id`* con l'ID del tuo account e *`dashboard-arn`* con l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid":
 "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. Esegui il `update-dashboard` comando per impostare e abilitare una pianificazione di aggiornamento configurando il parametro. `--refresh-schedule` Per la dashboard Highlights, l'unico valido `UNIT` è `HOURS` e l'unico valido `Value` è. 6

```
aws cloudtrail update-dashboard --dashboard-id AWSCloudTrail-Highlights \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

Visualizza le proprietà dei widget

Questa sezione descrive le proprietà di visualizzazione configurabili per i 4 tipi di visualizzazione: tabella, grafico a linee, grafico a torta e grafico a barre.

Tipi di visualizzazione:

- Tabella
- Grafico a linee
- Grafico a torta
- Grafico a barre

Tabella

L'esempio seguente mostra un widget configurato come tabella.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopErrors",
       "View": "Table"
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

La tabella seguente descrive le proprietà di visualizzazione configurabili per una tabella.

Parametro	Obbligatorio	Valore
`Height`	Sì	L'altezza della tabella in pollici.
`Width`	Sì	La larghezza della tabella in pollici.
`Title`	Sì	Il titolo della tabella.
`View`	Sì	Il tipo di visualizzazione del widget. Per una tabella, il valore è`Table`.

Grafico a linee

L'esempio seguente mostra un widget configurato come grafico a linee.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "AccountActivity",
```

```
        "View": "LineChart",
        "YAxisColumn": "eventCount",
        "XAxisColumn": "eventDate",
        "FilterColumn": "readOnly"
    },
    "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate, IF(readOnly,
 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE eventTime >
 '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly ORDER BY
 DATE_TRUNC('?', eventTime), readOnly",
    "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$", "$Period$"]
}
```

La tabella seguente descrive le proprietà di visualizzazione configurabili per un grafico a linee.

Parametro	Obbligatorio	Valore
`Height`	Sì	L'altezza del grafico a linee in pollici.
`Width`	Sì	La larghezza del grafico a linee in pollici.
`Title`	Sì	Il titolo del grafico a linee.
`View`	Sì	Il tipo di visualizzazione del widget. Per un grafico a linee, il valore è`LineChart` .
`YAxisColumn`	Sì	Il campo dei risultati della query che si desidera utilizzar e per la colonna dell'asse Y. Ad esempio, `eventCount` .
`XAxisColumn`	Sì	Il campo dei risultati della query che si desidera utilizzar e per la colonna dell'asse X. Ad esempio, `eventDate` .
`FilterColumn`	No	Il campo dei risultati della query in base al quale si

Parametro	Obbligatorio	Valore
		desidera filtrare. Ad esempio, `readOnly`.

Grafico a torta

L'esempio seguente mostra un widget configurato come grafico a torta.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "MostActiveRegions",
       "View": "PieChart",
       "LabelColumn": "awsRegion",
       "ValueColumn": "eventCount",
       "FilterColumn": "awsRegion"
    },
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

La tabella seguente descrive le proprietà di visualizzazione configurabili per un grafico a torta.

Parametro	Obbligatorio	Valore
`Height`	Sì	L'altezza del grafico a torta in pollici.
`Width`	Sì	La larghezza del grafico a torta in pollici.
`Title`	Sì	Il titolo del grafico a torta.
`View`	Sì	Il tipo di visualizzazione del widget. Per un grafico a torta, il valore è`PieChart`.

Parametro	Obbligatorio	Valore
`LabelColumn`	Sì	L'etichetta per i segmenti nel grafico a torta. Ad esempio, `awsRegion` .
`ValueColumn`	Sì	Il valore dei segmenti nel grafico a torta. Ad esempio, `ValueColumn` .
`FilterColumn`	No	Il campo dei risultati della query in base al quale si desidera filtrare. Ad esempio, `awsRegion` .

Grafico a barre

L'esempio seguente mostra un widget configurato come grafico a barre.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Horizontal"
    },
    "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
 COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

La tabella seguente descrive le proprietà di visualizzazione configurabili per un grafico a barre.

Parametro	Obbligatorio	Valore
`Height`	Sì	L'altezza del grafico a barre in pollici.
`Width`	Sì	La larghezza del grafico a barre in pollici.
`Title`	Sì	Il titolo del grafico a barre.
`View`	Sì	Il tipo di visualizzazione del widget. Per un grafico a barre, il valore è`BarChart`.
`LabelColumn`	Sì	L'etichetta per le barre nel grafico a barre. Ad esempio, `service`.
`ValueColumn`	Sì	Il valore delle barre nel grafico a barre. Ad esempio, `eventCount` .
`FilterColumn`	No	Il campo dei risultati della query in base al quale si desidera filtrare. Ad esempio, `service`.
`Orientation`	No	L'orientamento del grafico a barre, `Horizontal` o`Vertical`.

Gestisci i pannelli di controllo con AWS CLI

Questa sezione descrive diversi altri comandi che puoi eseguire per gestire i dashboard, tra cui creare una dashboard, elencare le dashboard, aggiornare una dashboard e aggiornare una dashboard.

Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro `--region` con il comando.

Esempi:

- Ottieni una dashboard con AWS CLI
- Elenca i dashboard con AWS CLI
- Allega una policy basata sulle risorse a un archivio dati di eventi o a un dashboard con AWS CLI
- Aggiorna manualmente una dashboard con AWS CLI
- Aggiorna un pannello di controllo con AWS CLI

Ottieni una dashboard con AWS CLI

Esegui il `get-dashboard` comando per restituire una dashboard. Specificare il `--dashboard-id` fornendo l'ARN del dashboard o il nome del dashboard.

```
aws cloudtrail get-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

Elenca i dashboard con AWS CLI

Esegui il `list-dashboards` comando per elencare le dashboard del tuo account.

- Includi il `--type` parametro, per visualizzare solo le `MANAGED` dashboard `CUSTOM` o.
- Includi il `--max-results` parametro per limitare il numero di risultati. I valori validi sono 1-100.
- `--name-prefix`Includi i dashboard di ritorno corrispondenti al prefisso specificato.

L'esempio seguente elenca tutti i dashboard.

```
aws cloudtrail list-dashboards
```

Questo esempio elenca solo i `CUSTOM` dashboard.

```
aws cloudtrail list-dashboards --type CUSTOM
```

L'esempio successivo elenca solo i `MANAGED` dashboard.

```
aws cloudtrail list-dashboards --type MANAGED
```

L'ultimo esempio elenca i dashboard che corrispondono al prefisso specificato.

```
aws cloudtrail list-dashboards --name-prefix ExamplePrefix
```

Allega una policy basata sulle risorse a un archivio dati di eventi o a un dashboard con AWS CLI

Esegui il `put-resource-policy` comando per applicare una policy basata sulle risorse a un data store o dashboard di eventi.

Allega una policy basata sulle risorse a un data store di eventi

Per eseguire interrogazioni su una dashboard durante un aggiornamento manuale o pianificato, è necessario allegare una policy basata sulle risorse a ogni archivio di dati di eventi associato a un widget sulla dashboard. Ciò consente a CloudTrail Lake di eseguire le query per tuo conto. Per ulteriori informazioni sulla politica basata sulle risorse, consulta. Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard

L'esempio seguente allega una policy basata sulle risorse a un archivio dati di eventi. Sostituiscilo *`account-id`* con l'ID del tuo account, *`eds-arn`* con l'ARN dell'archivio dati degli eventi per il quale CloudTrail verranno eseguite le query e con *`dashboard-arn`* l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartQuery", "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-
arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

Allega una policy basata sulle risorse a una dashboard

Per impostare una pianificazione di aggiornamento per una dashboard, devi allegare alla dashboard una policy basata sulle risorse per consentire a CloudTrail Lake di aggiornare la dashboard per tuo conto. Per ulteriori informazioni sulla politica basata sulle risorse, consulta. Esempio di policy basata sulle risorse per un pannello di controllo

L'esempio seguente allega una politica basata sulle risorse a un pannello di controllo. Sostituiscilo *`account-id`* con l'ID del tuo account e *`dashboard-arn`* con l'ARN della dashboard.

```
aws cloudtrail put-resource-policy \
```

```
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "DashboardPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartDashboardRefresh", "Condition": { "StringEquals": { "AWS:SourceArn":
 "dashboard-arn", "AWS:SourceAccount": "account-id"}}}]}'
```

Aggiorna manualmente una dashboard con AWS CLI

Esegui il `start-dashboard-refresh` comando per aggiornare manualmente la dashboard. Prima di poter eseguire questo comando, è necessario allegare una policy basata sulle risorse a ogni archivio di dati di eventi associato a un widget del dashboard.

L'esempio seguente mostra come aggiornare manualmente una dashboard personalizzata.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id  dashboard-id \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z"}'
```

L'esempio successivo mostra come aggiornare manualmente una dashboard gestita. Poiché i dashboard gestiti sono configurati da CloudTrail, la richiesta di aggiornamento deve includere l'ID del data store degli eventi su cui verranno eseguite le query.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id dashboard-id  \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z", "$EventDataStoreId
$": "eds-id"}'
```

Aggiorna un pannello di controllo con AWS CLI

Esegui il `update-dashboard` comando per aggiornare una dashboard. Puoi aggiornare la dashboard per impostare una pianificazione di aggiornamento, abilitare o disabilitare una pianificazione di aggiornamento, modificare i widget e abilitare o disabilitare la protezione dalla terminazione.

Aggiorna la pianificazione dell'aggiornamento con AWS CLI

L'esempio seguente aggiorna la pianificazione dell'aggiornamento per un pannello di controllo personalizzato denominato. `AccountActivityDashboard`

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status": "ENABLED"}'
```

Disabilita la protezione dalla terminazione e la pianificazione degli aggiornamenti su un pannello di controllo personalizzato con AWS CLI

L'esempio seguente disattiva la protezione dalla terminazione per un pannello di controllo personalizzato denominato in `AccountActivityDashboard` modo da consentire l'eliminazione del dashboard. Disattiva anche la pianificazione degli aggiornamenti.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{ "Status": "DISABLED"}' \
--no-termination-protection-enabled
```

Aggiungi un widget a una dashboard personalizzata

L'esempio seguente aggiunge un nuovo widget denominato `TopServices` alla dashboard personalizzata denominata`AccountActivityDashboard`. L'array di widget include i due widget già creati per la dashboard e il nuovo widget.

> **Note**
>
> In questo esempio, ? è racchiuso tra virgolette singole perché viene utilizzato con. `eventTime` A seconda del sistema operativo in uso, potrebbe essere necessario racchiudere le virgolette singole tra virgolette di escape. Per ulteriori informazioni, vedere Utilizzo di virgolette e letterali con stringhe in. AWS CLI

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
```

```
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Vertical"
      },
      "QueryStatement": "SELECT replace(eventSource, '.amazonaws.com') AS service,
 COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
  ]'
```

Eliminare un pannello di controllo con il AWS CLI

Questa sezione descrive come utilizzare il AWS CLI `delete-dashboard` comando per eliminare una dashboard di CloudTrail Lake.

Per eliminare un dashboard, specificalo `--dashboard-id` fornendo l'ARN del dashboard o il nome del dashboard.

```
aws cloudtrail delete-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

Se l'operazione riesce, non verrà generata alcuna risposta.

> **Note**
>
> Non puoi eliminare una dashboard se `--termination-protection-enabled` è impostata.

CloudTrail Domande sul lago

Le query in CloudTrail Lake sono create in SQL. È possibile creare una query nella scheda CloudTrail Lake Editor scrivendola da zero in SQL, aprendo una query salvata o di esempio e modificandola oppure utilizzando il generatore di query per produrre una query da un prompt in lingua inglese. Non è possibile sovrascrivere una query di esempio con le proprie modifiche, ma è possibile salvarla come nuova query. Per ulteriori informazioni sul linguaggio SQL consentito per le query, consultare CloudTrail Vincoli Lake SQL.

Una query illimitata (come ad esempio `SELECT * FROM edsID`) scansiona tutti i dati presenti nell'archivio di dati degli eventi. Per semplificare il controllo dei costi, consigliamo di vincolare le query aggiungendovi marche temporali `eventTime` di inizio e di fine. Di seguito è riportato un esempio che cerca tutti gli eventi in un datastore di eventi specificato in cui l'ora dell'evento è successiva (>) al 5 gennaio 2023 alle 13:51 e precedente (<) al 19 gennaio 2023 alle 13:51. Poiché un archivio di dati degli eventi ha un periodo di conservazione minimo di sette giorni, il tempo minimo tra l'inizio e la fine dei valori `eventTime` è di sette giorni.

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

Per informazioni su come ottimizzare le query, consulta. Ottimizza le query su Lake CloudTrail

Argomenti

- Strumenti dell'editor di query
- Crea query su CloudTrail Lake da istruzioni in linguaggio naturale
- Visualizza query di esempio con la console CloudTrail
- Crea o modifica un'interrogazione con la console CloudTrail
- Esegui una query e salva i risultati della query con la console

- Visualizza i risultati delle query con la console
- Riassumi i risultati delle interrogazioni in linguaggio naturale
- Scaricare i risultati della query salvati
- Validate CloudTrail Lake ha salvato i risultati delle query
- Ottimizza le query su Lake CloudTrail
- Esegui e gestisci le query di CloudTrail Lake con AWS CLI

Strumenti dell'editor di query

Una barra degli strumenti in alto a destra dell'editor di query offre dei comandi che consentono di creare e formattare la query SQL.

Di seguito sono elencati i comandi disponibili nella barra degli strumenti.

- Undo (Annulla): annulla l'ultima modifica del contenuto apportata nell'editor di query.
- Redo (Ripeti): ripristina l'ultima modifica del contenuto apportata nell'editor di query.
- Format selected (Formato selezionato): dispone il contenuto dell'editor di query in base alle convenzioni di formattazione e spaziatura di SQL.
- Commenta/decommenta selezionata: commenta la parte selezionata della query se non è già stata commentata. Se la parte selezionata è già commentata, la scelta di questa opzione rimuove il commento.

Crea query su CloudTrail Lake da istruzioni in linguaggio naturale

Puoi utilizzare il generatore di query CloudTrail Lake per produrre una query da un prompt in lingua inglese fornito da te. Il generatore di query utilizza l'intelligenza artificiale generativa (AI generativa) per produrre una query ready-to-use SQL dal prompt, che puoi quindi scegliere di eseguire nell'editor di query di Lake o perfezionarla ulteriormente. Non è necessario avere una conoscenza approfondita di SQL o dei campi di CloudTrail eventi per utilizzare il generatore di query.

Il prompt può essere una domanda o una dichiarazione sui dati degli eventi nel tuo archivio dati di eventi CloudTrail Lake. Ad esempio, puoi inserire istruzioni come e "What are my top errors in the past month?" “Give me a list of users that used SNS.”

Un prompt può contenere un minimo di 3 caratteri e un massimo di 500 caratteri.

Non sono previsti costi per la generazione di query; tuttavia, quando si eseguono query, vengono addebitati addebiti in base alla quantità di dati ottimizzati e compressi scansionati. Per aiutare a controllare i costi, si consiglia di limitare le query aggiungendo data e ora di inizio e fine alle query. `eventTime`

> **Note**
>
> Puoi fornire un feedback su una query generata scegliendo il pulsante pollice su o pollice giù che appare sotto la query generata. Quando fornisci un feedback, CloudTrail salva il prompt e la query generata.
> Non includete informazioni di identificazione personale, riservate o sensibili nelle vostre richieste.
> Questa funzionalità utilizza modelli di linguaggio generativi di intelligenza artificiale di grandi dimensioni (LLMs); consigliamo di ricontrollare la risposta LLM.

È possibile accedere al generatore di query utilizzando la CloudTrail console e. AWS CLI

CloudTrail console

Per utilizzare il generatore di query sulla CloudTrail console

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, in Lake, scegli Query.
3. Nella pagina Query, scegli la scheda Editor.
4. Scegliete il data store degli eventi per cui desiderate creare una query.
5. Nell'area del generatore di query, inserisci un prompt in inglese semplice. Per alcuni esempi, consulta Suggerimenti di esempio.
6. Scegliete Genera interrogazione. Il generatore di query tenterà di generare una query dal tuo prompt. In caso di successo, il generatore di query fornisce la query SQL nell'editor. Se la richiesta non ha esito positivo, riformula la richiesta e riprova.
7. (Facoltativo) Puoi fornire un feedback sulla query generata. Per fornire un feedback, scegli il pulsante pollice in su o pollice in giù che appare sotto la richiesta. Quando fornisci un feedback, CloudTrail salva il prompt e la query generata.
8. (Facoltativo) Scegliete Esegui per eseguire la query.

> **Note**
>
> Quando si eseguono le query, vengono addebitati costi in base alla quantità di dati ottimizzati e compressi scansionati. Per aiutare a controllare i costi, si consiglia di limitare le query aggiungendo data e ora di inizio e fine alle query. `eventTime`

9. (Facoltativo) Se si esegue la query e si ottengono risultati, è possibile scegliere Riepiloga risultati per generare un riepilogo dei risultati della query in linguaggio naturale in inglese. Questa opzione utilizza l'intelligenza artificiale generativa (AI generativa) per produrre il riepilogo. Per ulteriori informazioni su questa opzione, consulta Riassumi i risultati delle interrogazioni in linguaggio naturale.

   Puoi fornire un feedback sul riepilogo scegliendo il pulsante pollice su o pollice giù che appare sotto il riepilogo generato.

   > **Note**
   >
   > La funzionalità di riepilogo delle interrogazioni è disponibile in anteprima per CloudTrail Lake ed è soggetta a modifiche. Questa funzionalità è disponibile nelle seguenti regioni: Asia Pacifico (Tokyo), Stati Uniti orientali (Virginia settentrionale) e Stati Uniti occidentali (Oregon).

AWS CLI

Per generare un'interrogazione con AWS CLI

Eseguire il `generate-query` comando per generare una query da un prompt in inglese. Per `--event-data-stores`, fornisci l'ARN (o il suffisso ID dell'ARN) dell'archivio dati degli eventi su cui desideri eseguire la query. È possibile specificare un solo archivio dati di eventi. Per `--prompt`, fornisci il prompt in inglese.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

In caso di successo, il comando genera un'istruzione SQL e ne fornisce un'istruzione `QueryAlias` che verrà utilizzata con il `start-query` comando per eseguire la query sull'archivio dati degli eventi.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

Per eseguire una query con AWS CLI

Esegui il `start-query` comando con l'`QueryAlias`output del `generate-query` comando nell'esempio precedente. È inoltre possibile eseguire il `start-query` comando fornendo. `QueryStatement`

```
aws cloudtrail start-query --query-alias AWSCloudTrail-UUID
```

La risposta è una stringa `QueryId`. Per ottenere lo stato di una query, eseguire `describe-query` utilizzando il valore `QueryId` restituito da `start-query`. Se la query ha esito positivo, è possibile eseguire `get-query-results` per ottenere i risultati.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Le query che vengono eseguite per più di un'ora potrebbero scadere. È comunque possibile ottenere risultati parziali elaborati prima del timeout della query.
> Se stai inviando i risultati della query a un bucket S3 utilizzando il `--delivery-s3uri` parametro opzionale, la policy del bucket deve concedere l' CloudTrail autorizzazione a recapitare i risultati della query al bucket. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake.

Autorizzazioni richieste

Le politiche `AdministratorAccess`gestite `AWSCloudTrail_FullAccess`e quelle gestite forniscono entrambe le autorizzazioni necessarie per utilizzare questa funzionalità.

È inoltre possibile includere l'operazione `cloudtrail:GenerateQuery` in una policy inline o gestita dal cliente nuova o esistente.

Supporto delle Regioni

Questa funzionalità è supportata nei seguenti paesi: Regioni AWS

- Regione Asia Pacifico (Mumbai) (ap-south-1)
- Regione Asia Pacifico (Sydney) (ap-southeast-2)
- Regione Asia Pacifico (Tokyo) (ap-northeast-1)
- Regione Canada (Centrale) (ca-central-1)
- Regione Europa (Londra) (eu-west-2)
- Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Regione Stati Uniti occidentali (Oregon) (us-west-2)

Limitazioni

Di seguito sono riportate le limitazioni del generatore di query:

- Il generatore di query può accettare solo richieste in inglese.
- Il generatore di query può generare solo query per archivi di dati di eventi che raccolgono CloudTrail eventi (eventi di gestione, eventi di dati, eventi di attività di rete).
- Il generatore di query non può generare query per prompt che non riguardano i dati degli eventi di Lake. CloudTrail

Suggerimenti di esempio

Questa sezione fornisce istruzioni di esempio e le query SQL risultanti generate dai prompt.

Se scegli di eseguire le query di esempio in questa sezione, sostituiscile *`eds-id`* con l'ID del data store degli eventi su cui desideri interrogare e sostituisci i timestamp con i timestamp appropriati per il tuo caso d'uso. I timestamp hanno il seguente formato:. `YYYY-MM-DD HH:MM:SS`

Richiesta: What are my top errors in the past month?

Interrogazione SQL:

```
SELECT
    errorMessage,
    COUNT(*) as eventCount
FROM
    eds-id
WHERE
    errorMessage IS NOT NULL
AND eventTime >= timestamp '2024-05-01 00:00:00'
AND eventTime <= timestamp '2024-05-31 23:59:59'
GROUP BY 1
ORDER BY 2 DESC
LIMIT 2;
```

Richiesta: Give me a list of users that used Amazon SNS.

Interrogazione SQL:

```
SELECT
    DISTINCT userIdentity.arn AS user
FROM
    eds-id
WHERE
    eventSource = 'sns.amazonaws.com'
```

Richiesta: What are my API counts each day for read and write events in the past month?

Interrogazione SQL:

```
SELECT date(eventTime) AS event_date,
    SUM(
        CASE
            WHEN readonly = true THEN 1
            ELSE 0
        END
    ) AS read_events,
    SUM(
        CASE
            WHEN readonly = false THEN 1
```

```
            ELSE 0
        END
    ) AS write_events
FROM
    eds-id
WHERE
    eventTime >= timestamp '2024-05-04 00:00:00'
AND eventTime <= timestamp '2024-06-04 23:59:59'
GROUP BY 1
ORDER BY 1 ASC;
```

Richiesta: Show any events with access denied errors for the past three weeks.

Interrogazione SQL:

```
SELECT *
FROM
  eds-id
WHERE
  WHERE (errorCode = 'AccessDenied' OR errorMessage = 'Access Denied')
AND eventTime >= timestamp '2024-05-16 01:00:00'
AND eventTime <= timestamp '2024-06-06 01:00:00'
```

Richiesta: Query the number of calls each operator performed on the date 2024-05-01. The operator is a principal tag.

Interrogazione SQL:

```
SELECT element_at(
        eventContext.tagContext.principalTags,
        'operator'
    ) AS operator,
    COUNT(*) AS eventCount
FROM
    eds-id
WHERE eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
GROUP BY 1
ORDER BY 2 DESC;
```

Richiesta: Give me all event IDs that touched resources within the AWS CloudFormation stack with name myStack on the date 2024-05-01.

Interrogazione SQL:

```
SELECT eventID
FROM
    eds-id
WHERE any_match(
        eventContext.tagcontext.resourcetags,
        rt->element_at(rt.tags, 'aws:cloudformation:stack-name') = 'myStack'
    )
    AND eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
```

Richiesta: Count the number of events grouped by resource tag 'solution' values, listing them in descending order of count.

Interrogazione SQL:

```
SELECT element_at(rt.tags, 'solution'),
    count(*) as event_count
FROM
    eds-id,
    unnest(eventContext.tagContext.resourceTags) as rt
WHERE eventtime < '2025-05-14 19:00:00'
GROUP BY 1
ORDER BY 2 DESC;
```

Richiesta: Find all Amazon S3 data events where resource tag Environment has value prod.

Interrogazione SQL:

```
SELECT *
FROM
    eds-id
WHERE eventCategory = 'Data'
    AND eventSource = 's3.amazonaws.com'
    AND eventtime >= '2025-05-14 00:00:00'
    AND eventtime < '2025-05-14 20:00:00'
    AND any_match(
        eventContext.tagContext.resourceTags,
        rt->element_at(rt.tags, 'Environment') = 'prod'
    )
```

Visualizza query di esempio con la console CloudTrail

La CloudTrail console fornisce una serie di query di esempio che possono aiutarti a iniziare a scrivere le tue query.

CloudTrail Le query comportano addebiti in base alla quantità di dati scansionati. Per semplificare il controllo dei costi, consigliamo di vincolare le query aggiungendovi marche temporali `eventTime` di inizio e di fine. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

> **Note**
>
> Puoi anche visualizzare le query create dalla GitHub community. Per ulteriori informazioni, consulta CloudTrailLake sample queries sul GitHub sito Web. AWS CloudTrail non ha valutato le interrogazioni in. GitHub

Visualizzazione ed esecuzione di una query di esempio

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
2. Dal pannello di navigazione, in Lake, scegli Query.
3. Nella pagina Query, scegli la scheda Sample queries (Query di esempio).
4. Scegli una query di esempio dall'elenco o inserisci una frase in base alla quale effettuare la ricerca. In questo esempio, apriremo la query Indaga chi ha apportato modifiche alla console scegliendo il nome della query. La query viene visualizzata nella scheda Editor.

   > **Note**
   >
   > Per impostazione predefinita, questa pagina utilizza la funzionalità di ricerca di base. È possibile migliorare la funzionalità di ricerca aggiungendo le autorizzazioni per l'`cloudtrail:SearchSampleQueries`azione, se non sono già previste dalla politica in materia di autorizzazioni. La politica `AWSCloudTrail_FullAccess`gestita fornisce le autorizzazioni per eseguire l'azione. `cloudtrail:SearchSampleQueries`

5. Nella scheda Editor, scegli il datastore di eventi per il quale desideri eseguire la query. Quando si sceglie l'Event Data Store dall'elenco, compila CloudTrail automaticamente l'ID dell'Event Data Store nella `FROM` riga dell'editor di query.

6. Per eseguire la query, scegli Esegui.

   La scheda Output del comando mostra i metadati relativi alla query, ad esempio se la query ha avuto esito positivo, il numero di record corrispondenti e la durata di esecuzione della query.

   La scheda Risultati della query mostra i dati degli eventi nel datastore di eventi selezionato che corrispondono alla query.

Per ulteriori informazioni sulla modifica di una query, consulta Crea o modifica un'interrogazione con la console CloudTrail . Per ulteriori informazioni sull'esecuzione di una query e sul salvataggio dei relativi risultati, consulta Esegui una query e salva i risultati della query con la console.

Crea o modifica un'interrogazione con la console CloudTrail

In questa procedura dettagliata, apriamo una delle query di esempio, la modifichiamo per trovare le azioni intraprese da un utente specifico denominato `Alice` e la salviamo come nuova query. È possibile modificare una query salvata anche nella scheda Saved queries (Query salvate), se ne hai salvata qualcuna. Per semplificare il controllo dei costi, consigliamo di vincolare le query aggiungendovi marche temporali `eventTime` di inizio e di fine.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, in Lake, scegli Query.
3. Nella pagina Query, scegli la scheda Sample queries (Query di esempio).
4. Apri una query di esempio selezionando il nome della query. La query viene visualizzata nella scheda Editor. In questo esempio, selezioneremo la query denominata Indaga azioni utente e modificheremo la query per trovare le azioni per un utente specifico denominato `Alice`.
5. Nella scheda Editor, modifica la riga `WHERE` per specificare l'utente che desideri esaminare e aggiorna i valori di `eventTime` in base alle necessità. Il valore di `FROM` è la parte ID dell'ARN dell'Event Data Store e viene compilato automaticamente da CloudTrail quando si sceglie l'Event Data Store.

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Per verificare che la query funzioni, prima di salvarla è possibile eseguirla. Per eseguire una query, scegliere un archivio di dati degli eventi dall'elenco a discesa Event data store (Archivi di dati degli eventi), quindi scegliere Run (Esegui). Consultare la colonna Status (Stato) della scheda Command output (Output dei comandi) per la query attiva per verificare che sia stata eseguita correttamente.
7. Dopo aver aggiornato la query di esempio, scegli Salva
8. In Save query (Salva la query), inserire un nome e una descrizione per la query. Scegliere Save query (Salva la query) per salvare le modifiche come nuova query. Per eliminare le modifiche apportate a una query, scegliere Cancel (Annulla) oppure chiudere la finestra Save query (Salva la query).

> **Note**
>
> Le interrogazioni salvate sono collegate al browser; se si utilizza un browser diverso o un dispositivo diverso per accedere alla CloudTrail console, le query salvate non sono disponibili.

9. Aprire la scheda Saved queries (Query salvate) per visualizzare la nuova query nella tabella.

Esegui una query e salva i risultati della query con la console

Dopo avere scelto o salvato una query, è possibile eseguirla in un archivio di dati degli eventi.

Quando si esegue query, è possibile salvare i risultati della query in un bucket Amazon S3. Quando esegui delle query in CloudTrail Lake, ti vengono addebitati dei costi in base alla quantità di dati analizzati dalla query. Non sono previsti costi aggiuntivi per CloudTrail Lake per il salvataggio dei

risultati delle query in un bucket S3, tuttavia sono previsti costi di archiviazione S3. Per ulteriori informazioni sui prezzi, consultare Prezzi di Amazon S3.

Quando si salvano i risultati delle query, i risultati delle query possono essere visualizzati nella CloudTrail console prima di essere visualizzati nel bucket S3, in quanto CloudTrail fornisce i risultati delle query dopo il completamento della scansione delle query. Sebbene la maggior parte delle query venga completata in pochi minuti, a seconda delle dimensioni dell'archivio dati degli eventi, la consegna dei risultati delle query CloudTrail al bucket S3 può richiedere molto più tempo. CloudTrail fornisce i risultati delle query al bucket S3 in formato gzip compresso. In media, al termine della scansione delle query, è possibile aspettarsi una latenza di 60-90 secondi per ogni GB di dati consegnato al bucket S3.

Per eseguire una query utilizzando Lake CloudTrail

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Dal pannello di navigazione, in Lake, scegli Query.
3. Nelle schede Query salvate o Query di esempio, scegli una query da eseguire selezionando il valore in Nome query.
4. Nella scheda Editor, per Event data store (Archivio di dati degli eventi) scegliere un archivio di dati degli eventi dall'elenco a discesa.
5. (Opzionale) Nella scheda Editor, scegliere Save results to S3 (Salva risultati su S3) per salvare i risultati della query in un bucket S3. Quando scegli il bucket S3 predefinito, CloudTrail crea e applica le politiche di bucket richieste. Se scegli il bucket S3 predefinito, la tua policy IAM deve includere l'autorizzazione per l'`s3:PutEncryptionConfigurationazione` perché per impostazione predefinita è abilitata la crittografia lato server per il bucket. Per ulteriori informazioni sui risultati della query, consultare Ulteriori informazioni sui risultati della query salvati.

> **Note**
>
> Per utilizzare un bucket diverso, specificare il nome del bucket o scegliere Browse S3 (Sfoglia S3) per scegliere un bucket. La policy del bucket deve concedere l' CloudTrail autorizzazione a fornire i risultati delle query al bucket. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake.

6. Nella scheda Editor (Modifica), scegliere Run (Esegui).

   A seconda delle dimensioni dell'archivio di dati degli eventi e del numero di giorni di dati inclusi, l'esecuzione di una query può richiedere diversi minuti. La scheda Command output (Output dei comandi) mostra lo stato di una query e se l'esecuzione è terminata. Quando l'esecuzione di una query è terminata, aprire la scheda Query results (Risultati della query) per visualizzare una tabella dei risultati per la query attiva (quella attualmente visualizzata nell'editor).

> **Note**
>
> Le query che vengono eseguite per più di un'ora potrebbero scadere. È comunque possibile ottenere risultati parziali elaborati prima della scadenza della query. CloudTrail non fornisce risultati parziali delle query a un bucket S3. Per evitare un timeout, è possibile perfezionare la propria query per limitare la quantità di dati scansionati specificando un intervallo di tempo più ristretto.

Ulteriori informazioni sui risultati della query salvati

Dopo aver salvato i risultati della query, è possibile scaricare i risultati della query salvate dal bucket S3. Per ulteriori informazioni su come trovare e scaricare i risultati della query salvati, consultare Scaricare i risultati della query salvati.

È inoltre possibile convalidare i risultati delle query salvate per determinare se i risultati delle query sono stati modificati, eliminati o invariati dopo la CloudTrail consegna dei risultati della query. Per ulteriori informazioni sulla convalida dei risultati della query salvati, consultare Validate CloudTrail Lake ha salvato i risultati delle query.

Esempio: salvare i risultati delle query in un bucket Amazon S3

Questa procedura dettagliata mostra come salvare i risultati delle query in un bucket S3 e quindi scaricarli.

Salvataggio dei risultati della query in un bucket Amazon S3

1. Accedi a AWS Management Console e apri la console all'indirizzo. CloudTrail https://console.aws.amazon.com/cloudtrail/
2. Dal pannello di navigazione, in Lake, scegli Query.

3. Nelle schede Query salvate o Query di esempio, scegli una query da eseguire selezionando il valore in Nome query. In questo esempio, sceglieremo la query di esempio denominata Indaga azioni utente.
4. Nella scheda Editor, per Event data store (Archivio di dati degli eventi) scegliere un archivio di dati degli eventi dall'elenco a discesa. Quando scegli l'Event Data Store dall'elenco, compila CloudTrail automaticamente l'ID dell'Event Data Store nella `From` riga.
5. In questa query di esempio, modificheremo il valore di `userIdentity.`ARN per specificare un utente denominato `Admin` e lasceremo i valori predefiniti per `eventTime`. Quando si esegue una query, viene addebitata la quantità di dati scansionati. Per semplificare il controllo dei costi, consigliamo di vincolare le query aggiungendovi marche temporali `eventTime` di inizio e di fine.
6. Scegli Salva risultati in S3 per salvare i risultati della query in un bucket S3. Quando scegli il bucket S3 predefinito, CloudTrail crea e applica le politiche di bucket richieste. Se scegli il bucket S3 predefinito, la tua policy IAM deve includere l'autorizzazione per l'`s3:PutEncryptionConfigurationazione` perché per impostazione predefinita è abilitata la crittografia lato server per il bucket. In questo esempio, utilizzeremo il bucket S3 predefinito.

   > **Note**
   >
   > Per utilizzare un bucket diverso, specificare il nome del bucket o scegliere Browse S3 (Sfoglia S3) per scegliere un bucket. La policy del bucket deve concedere l' CloudTrail autorizzazione a fornire i risultati delle query al bucket. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake.

7. Seleziona Esegui. A seconda delle dimensioni dell'archivio di dati degli eventi e del numero di giorni di dati inclusi, l'esecuzione di una query può richiedere diversi minuti. La scheda Command output (Output dei comandi) mostra lo stato di una query e se l'esecuzione è terminata. Quando l'esecuzione di una query è terminata, aprire la scheda Query results (Risultati della query) per visualizzare una tabella dei risultati per la query attiva (quella attualmente visualizzata nell'editor).
8. Una volta CloudTrail completata la consegna dei risultati delle query salvate nel bucket S3, la colonna Delivery status fornisce un collegamento al bucket S3 che contiene i file dei risultati delle query salvate e un file di segno che è possibile utilizzare per verificare i risultati delle query

salvate. Scegli Visualizza in S3 per visualizzare i file dei risultati delle query e i file di firma nel bucket S3.

> **Note**
>
> Quando salvi i risultati delle query, i risultati delle query possono essere visualizzati nella CloudTrail console prima di essere visualizzati nel bucket S3, in quanto CloudTrail fornisce i risultati della query dopo il completamento della scansione della query. Sebbene la maggior parte delle query venga completata in pochi minuti, a seconda delle dimensioni dell'archivio dati degli eventi, la consegna dei risultati delle query CloudTrail al bucket S3 può richiedere molto più tempo. CloudTrail fornisce i risultati delle query al bucket S3 in formato gzip compresso. In media, al termine della scansione delle query, è possibile aspettarsi una latenza di 60-90 secondi per ogni GB di dati consegnato al bucket S3.

9. Per scaricare i risultati della query, scegli il file dei risultati della query (in questo esempio, `result_1.csv.gz`), quindi scegli Scarica.

Per ulteriori informazioni sulla convalida dei risultati della query salvati, consulta Validate CloudTrail Lake ha salvato i risultati delle query.

Visualizza i risultati delle query con la console

Al termine dell'esecuzione della query, è possibile visualizzarne i risultati. I risultati di una query sono disponibili per sette giorni dopo l'esecuzione della stessa. È possibile visualizzare i risultati della query attiva nella scheda Query results (Risultati della query) oppure è possibile accedere ai risultati di tutte le query recenti nella scheda Results history (Cronologia dei risultati) sulla pagina iniziale di Lake.

I risultati della query possono variare da un'esecuzione all'altra, poiché è possibile che eventi successivi siano registrati nel periodo che intercorre tra le query.

Quando si salvano i risultati delle query, i risultati delle query possono essere visualizzati nella CloudTrail console prima di essere visualizzati nel bucket S3, poiché CloudTrail fornisce i risultati della query dopo il completamento della scansione della query. Sebbene la maggior parte delle

query venga completata in pochi minuti, a seconda delle dimensioni dell'archivio dati degli eventi, la consegna dei risultati delle query CloudTrail al bucket S3 può richiedere molto più tempo. CloudTrail fornisce i risultati delle query al bucket S3 in formato gzip compresso. In media, una volta completata la scansione delle query, puoi aspettarti una latenza compresa tra 60 e 90 secondi per ogni GB di dati fornito al bucket S3. Per ulteriori informazioni su come trovare e scaricare i risultati della query salvati, consultare Scaricare i risultati della query salvati.

> **Note**
>
> Le query che vengono eseguite per più di un'ora potrebbero scadere. È comunque possibile ottenere risultati parziali elaborati prima della scadenza della query. CloudTrail non fornisce risultati parziali delle query a un bucket S3. Per evitare un timeout, è possibile perfezionare la propria query per limitare la quantità di dati scansionati specificando un intervallo di tempo più ristretto.

Per visualizzare i risultati delle query

1. Scegli la scheda Risultati delle interrogazioni nell'editor delle query se non è già selezionata. Nella scheda Query results (Risultati della query) per una query attiva, ogni riga rappresenta il risultato di un evento corrispondente alla query. Filtrare i risultati inserendo tutto o parte di un valore del campo dell'evento nella barra di ricerca. Per copiare un evento, scegli l'evento desiderato, quindi seleziona Copia.
2. (Facoltativo) Scegliete Riepiloga risultati per generare un riepilogo in linguaggio naturale dei risultati della query. Il riepilogo è fornito in inglese. Questa opzione utilizza l'intelligenza artificiale generativa (AI generativa) per produrre il riepilogo. Per ulteriori informazioni su questa opzione, consulta Riassumi i risultati delle interrogazioni in linguaggio naturale.

   Puoi fornire un feedback sul riepilogo scegliendo il pulsante pollice su o pollice giù che appare sotto il riepilogo generato.

   > **Note**
   >
   > La funzionalità di riepilogo delle interrogazioni è disponibile in anteprima per CloudTrail Lake ed è soggetta a modifiche. Questa funzionalità è disponibile nelle seguenti regioni: Asia Pacifico (Tokyo), Stati Uniti orientali (Virginia settentrionale) e Stati Uniti occidentali (Oregon).

3. Nella scheda Command output (Output dei comandi) è possibile visualizzare i metadati relativi alla query eseguita, ad esempio l'ID dell'archivio di dati degli eventi, il tempo di esecuzione, il numero di risultati acquisiti e se la query ha avuto esito positivo o meno. Se i risultati della query sono stati in un bucket Amazon S3, i metadati includono anche un collegamento al bucket S3 contenente i risultati della query salvati.

Riassumi i risultati delle interrogazioni in linguaggio naturale

> **Note**
>
> La funzionalità di riepilogo delle interrogazioni è disponibile in anteprima per CloudTrail Lake ed è soggetta a modifiche.

Al termine della query, è possibile ottenere un riepilogo dei risultati della query in linguaggio naturale dalla scheda Risultati della query nell'editor delle query. Questa opzione utilizza l'intelligenza artificiale generativa (AI generativa) per produrre il riepilogo.

Per riepilogare i risultati delle interrogazioni

1. Dalla scheda Risultati della query dell'editor di query, scegli Riepiloga risultati per generare un riepilogo in linguaggio naturale dei risultati della query. Il riepilogo è fornito in inglese.
2. (Facoltativo) Fornisci un feedback sul riepilogo scegliendo il pulsante pollice su o pollice giù che appare sotto il riepilogo generato.

Se il relativo archivio dati degli eventi è crittografato utilizzando una chiave KMS, non è possibile utilizzare la chiave KMS per crittografare i risultati e il riepilogo della query. I risultati e il riepilogo della query vengono invece crittografati da. CloudTrail

L'accesso al riepilogo generato è autorizzato in base alle autorizzazioni `GetQueryResultsGenerateQueryResultsSummary`, e KMS (se il relativo archivio di date degli eventi è crittografato con una chiave KMS). Quando viene generato un riepilogo, CloudTrail registra un evento denominato `GenerateQueryResultsSummary` per la visibilità.

Autorizzazioni richieste

Le politiche `AdministratorAccess`gestite `AWSCloudTrail_FullAccess`e quelle gestite forniscono entrambe le autorizzazioni necessarie per utilizzare questa funzionalità.

Puoi anche includere le `cloudtrail:GetQueryResults` azioni `cloudtrail:GenerateQueryResultsSummary` e in una politica in linea o gestita dal cliente nuova o esistente.

Se l'archivio dati degli eventi relativo al riepilogo dei risultati della query è crittografato con una chiave KMS, sono necessarie anche le autorizzazioni per la chiave KMS.

Supporto delle Regioni

Questa funzionalità è disponibile nelle seguenti versioni: Regioni AWS

- Regione Asia Pacifico (Tokyo) (ap-northeast-1)
- Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Regione Stati Uniti occidentali (Oregon) (us-west-2)

Limitazioni

Di seguito sono riportate le limitazioni di questa funzionalità:

- I riepiloghi sono disponibili solo in inglese.
- I riepiloghi sono limitati agli archivi di dati sugli eventi che raccolgono CloudTrail eventi (eventi di gestione, eventi sui dati, eventi di attività di rete).
- Ogni riepilogo contiene i risultati di una singola interrogazione.
- La dimensione dei risultati della query deve essere inferiore a 250 KB.
- La quota mensile di risultati delle query che possono essere riepilogati è di 3 MB.

Scaricare i risultati della query salvati

Dopo aver salvato i risultati della query, devi essere in grado di individuare il file contenente i risultati della query. CloudTrail invia i risultati delle query a un bucket Amazon S3 specificato al momento del salvataggio dei risultati della query.

> **Note**
>
> Quando salvi i risultati della query, i risultati della query possono essere visualizzati nella console prima di essere visualizzati nel bucket S3, poiché CloudTrail fornisce i risultati della query dopo il completamento della scansione della query. Sebbene la maggior parte delle

query venga completata in pochi minuti, a seconda delle dimensioni dell'archivio dati degli eventi, la consegna dei risultati delle query CloudTrail al bucket S3 può richiedere molto più tempo. CloudTrail fornisce i risultati delle query al bucket S3 in formato gzip compresso. In media, al termine della scansione delle query, è possibile aspettarsi una latenza di 60-90 secondi per ogni GB di dati consegnato al bucket S3.

Argomenti

- Trova i risultati delle query salvate CloudTrail su Lake
- Scarica i risultati delle query salvate su CloudTrail Lake

Trova i risultati delle query salvate CloudTrail su Lake

CloudTrail pubblica i risultati delle query e firma i file nel tuo bucket S3. Il file dei risultati della query contiene l'output della query salvata e il file dei segni fornisce la firma e il valore hash per i risultati della query. Per convalidare i risultati della query, è possibile utilizzare il file di firma. Per ulteriori informazioni sui risultati della query, consultare Validate CloudTrail Lake ha salvato i risultati delle query.

Per recuperare un file dei risultati della query, è possibile utilizzare la console Amazon S3, l'interfaccia a riga di comando (Command Line Interface, CLI) o l'API Amazon S3.

Per trovare i risultati della query mediante la console Amazon S3

1. Apri la console Amazon S3.
2. Scegliere il bucket specificato.
3. Esplorare la gerarchia di oggetti fino a trovare i file dei risultati della query e di firma desiderati. Il file dei risultati della query ha un'estensione .csv.gz e il file di firma ha un'estensione .json.

Sarà possibile navigare in una gerarchia di oggetti simile a quella dell'esempio seguente, ma con valori diversi per nome di bucket, ID account, regione e data.

```
All Buckets
    amzn-s3-demo-bucket
        AWSLogs
            Account_ID;
                CloudTrail-Lake
```

```
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Scarica i risultati delle query salvate su CloudTrail Lake

Quando salvi i risultati delle query, CloudTrail invia due tipi di file al tuo bucket Amazon S3.

- Un file di firma in formato JSON che è possibile utilizzare per convalidare i file dei risultati della query. Il file di firma è denominato result_sign.json. Per ulteriori informazioni sul file di firma, consultare CloudTrail struttura del file di firma.
- Uno o più file dei risultati della query in formato CSV, che contengono i risultati della query. Il numero di file dei risultati della query consegnati dipende dalla dimensione totale dei risultati della query. Le dimensioni massime del file per un file dei risultati della query sono di 1 TB. Ogni file dei risultati della query è denominato *number* result_ .csv.gz. Ad esempio, se la dimensione totale dei risultati della query fosse di 2 TB, si avrebbero due file dei risultati della query, result_1.csv.gz e result_2.csv.gz.

CloudTrail i file dei risultati delle query e dei segni sono oggetti Amazon S3. Puoi utilizzare la console S3, AWS Command Line Interface (CLI) o l'API S3 per recuperare i risultati delle query e firmare i file.

La procedura seguente descrive come scaricare i file dei risultati della query e di firma mediante la console Amazon S3.

Per scaricare il proprio file dei risultati della query o di firma mediante la console Amazon S3

1. Apri la console Amazon S3.
2. Scegliere il bucket e scegliere il file da scaricare.
3. Scegliere Download (Scarica) e seguire le istruzioni per salvare il file.

> **Note**
>
> Alcuni browser, ad esempio Chrome, estraggono automaticamente il file dei risultati della query per conto dell'utente. Se il browser esegue automaticamente questa operazione, passare al punto 5.

4. Utilizzare un prodotto, ad esempio 7-Zip, per estrarre i file dei risultati della query.
5. Aprire il file dei risultati della query o di firma.

Validate CloudTrail Lake ha salvato i risultati delle query

Per determinare se i risultati della query sono stati modificati, eliminati o invariati dopo aver CloudTrail fornito i risultati della query, è possibile utilizzare la convalida dell'integrità dei risultati delle CloudTrail query. Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file dei risultati delle query senza essere rilevati. CloudTrail Per convalidare i file dei risultati della query, è possibile utilizzare la riga di comando.

Perché utilizzare questa funzionalità?

I file dei risultati della query convalidati sono preziosi nelle indagini giudiziarie e sulla sicurezza. Ad esempio, un file dei risultati della query convalidato consente di affermare in modo positivo che il file dei risultati della query stesso non è cambiato. Il processo di convalida dell'integrità del file dei risultati della CloudTrail query consente inoltre di sapere se un file dei risultati della query è stato eliminato o modificato.

Argomenti

- Convalida i risultati delle interrogazioni salvate con AWS CLI
- CloudTrail struttura del file di firma
- Implementazioni personalizzate della convalida dell'integrità dei file dei risultati delle CloudTrail query

Convalida i risultati delle interrogazioni salvate con AWS CLI

È possibile convalidare l'integrità dei file del risultato della query e firmare il file utilizzando il comando aws cloudtrail verify-query-results.

Prerequisiti

Per convalidare l'integrità dei risultati della query con la riga di comando, è necessario che siano soddisfatte le seguenti condizioni:

- È necessario disporre di una connettività online a. AWS

- È necessario utilizzare AWS CLI la versione 2.
- Per convalidare i file dei risultati delle query e firmare il file in locale, si applicano le seguenti condizioni:
  - È necessario inserire i file dei risultati della query e il file di firma nel percorso del file specificato. Specifica il percorso del file come valore per il parametro --local-export-path.
  - Non è necessario rinominare i file dei risultati della query e il file di firma.
- Per convalidare i file dei risultati delle query e firmare il file nel bucket S3, si applicano le seguenti condizioni:
  - Non è necessario rinominare i file dei risultati della query e il file di firma.
  - È necessario disporre dell'accesso in lettura al bucket Amazon S3 contenente i file di firma e dei risultati della query.
  - Il prefisso S3 specificato deve contenere i file dei risultati della query e il file di firma. Specifica il prefisso S3 come valore per il parametro --s3-prefix.

verify-query-results

Il comando verify-query-results verifica il valore hash di ogni file dei risultati della query confrontando il valore con il `fileHashValue` nel file di firma e quindi convalidando `hashSignature` nel file di firma.

Quando verifichi i risultati della query, puoi utilizzare le opzioni della riga di comando --s3-bucket e --s3-prefix per convalidare i file dei risultati delle query e il file di firma archiviati in un bucket S3, oppure puoi utilizzare l'opzione della riga di comando --local-export-path per eseguire una convalida locale dei file dei risultati delle query e del file di firma scaricati.

> **Note**
>
> Il comando verify-query-results è specifico della Regione. È necessario specificare l'opzione --region globale per convalidare i risultati della query per uno specifico Regione AWS.

Di seguito sono elencate le opzioni per il comando verify-query-results.

--s3-bucket *<string>*

Specifica il nome del bucket S3 che memorizza i file dei risultati della query e il file di firma. Non è possibile utilizzare questo parametro con --local-export-path.

--s3-prefix *<string>*

Specifica il percorso S3 della cartella S3 che contiene i file dei risultati delle query e il file di firma (ad esempio, `s3/path/`). Non è possibile utilizzare questo parametro con --local-export-path. Non è necessario fornire questo parametro se i file si trovano nella directory root del bucket S3.

--local-export-path *<string>*

Specifica la directory locale che contiene i file dei risultati delle query e il file di firma (ad esempio, `/local/path/to/export/file/`). Non è possibile utilizzare questo parametro con --s3-bucket o --s3-prefix.

Esempi

L'esempio seguente convalida i risultati delle query utilizzando le opzioni della riga di comando --s3-bucket e --s3-prefix per specificare il nome del bucket S3 e il prefisso contenente i file dei risultati delle query e il file di firma.

```
aws cloudtrail verify-query-results --s3-bucket amzn-s3-demo-bucket --s3-prefix prefix
 --region region
```

L'esempio seguente convalida i risultati delle query scaricati utilizzando l'opzione della riga di comando --local-export-path per specificare il percorso locale dei file dei risultati della query e del file di firma. Per informazioni sul download dei file dei risultati delle query, consulta Scarica i risultati delle query salvate su CloudTrail Lake.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

Risultati della convalida

Nella tabella riportata di seguito sono descritti i possibili messaggi di convalida per i file dei risultati della query e il file di firma.

Tipo di file	Messaggio di convalida	Descrizione
`Sign file`	`Successfully validated sign and query result files`	La firma del file di firma è valida. I file dei risultati della query a cui fa riferimento possono essere controllati.

Tipo di file	Messaggio di convalida	Descrizione
`Query result file`	`ValidationError: "File` *`file_name`* `has inconsistent hash value with hash value recorded in sign file, hash value in sign file is` *`expected_hash`* `, but get` *`computed_hash`*	La convalida non è riuscita perché il valore hash per il file dei risultati della query non corrisponde al `fileHashValue` nel file di firma.
`Sign file`	`ValidationError: Invalid signature in sign file`	La convalida del file di firma non è riuscita perché la firma non è valida.

CloudTrail struttura del file di firma

Il file di firma contiene il nome di ogni file dei risultati della query distribuito nel bucket Amazon S3 al momento del salvataggio dei risultati della query, il valore hash per ogni file dei risultati della query e la firma digitale del file. I valori di firma digitale e hash vengono utilizzati per convalidare l'integrità del file dei risultati della query e del file di firma stesso.

Posizione del file di firma

Il file di firma viene distribuito in un bucket Amazon S3 il cui percorso è conforme alla seguente sintassi.

```
s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Contenuto dei file di firma di esempio

Il seguente file sign di esempio contiene informazioni per i risultati delle query di CloudTrail Lake.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
```

```
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

Descrizione dei campi del file di firma

Di seguito sono riportate descrizioni di ciascun campo del file di firma:

`version`

La versione del file di firma.

`region`

La regione dell' AWS account utilizzato per salvare i risultati della query.

`files.fileHashValue`

Valore hash con codifica esadecimale del contenuto compresso del file dei risultati della query.

`files.fileName`

Il nome del file dei risultati della query.

`hashAlgorithm`

Algoritmo hash utilizzato per eseguire l'hashing del file dei risultati della query.

`signatureAlgorithm`

Algoritmo utilizzato per firmare il file di firma.

`queryCompleteTime`

Indica quando i risultati della query sono CloudTrail stati consegnati al bucket S3. È possibile utilizzare questo valore per trovare la chiave pubblica.

`hashSignature`

La firma hash per il file.

`publicKeyFingerprint`

L'impronta con codifica esadecimale della chiave pubblica utilizzata per firmare il file di firma.

Implementazioni personalizzate della convalida dell'integrità dei file dei risultati delle CloudTrail query

Poiché CloudTrail utilizza algoritmi crittografici e funzioni hash standard del settore e disponibili apertamente, è possibile creare strumenti personalizzati per convalidare l'integrità dei file dei risultati delle query. CloudTrail Quando salvi i risultati delle query in un bucket Amazon S3, CloudTrail invia un file di firma al bucket S3. È possibile implementare una soluzione di convalida personalizzata per convalidare la firma e i file dei risultati della query. Per ulteriori informazioni sul file di firma, consultare CloudTrail struttura del file di firma.

Questo argomento descrive come viene firmato il file e illustra in dettaglio le procedure necessarie per implementare una soluzione che convalida il file di firma e i file dei risultati della query a cui il file di firma fa riferimento.

Comprendere come CloudTrail vengono firmati i file di firma

CloudTrail i file di firma sono firmati con firme digitali RSA. Per ogni file di firma, CloudTrail effettua le seguenti operazioni:

1. Crea una lista hash contenente il valore hash per ogni file dei risultati della query.
2. Recupera una chiave privata univoca per la Regione.
3. Passa l'hash SHA-256 della stringa e la chiave privata all'algoritmo di firma RSA, che genera una firma digitale.
4. Codifica il codice byte della firma in formato esadecimale.
5. Inserisce la firma digitale nel file di firma.

Contenuto della stringa di firma dei dati

La stringa di firma dei dati è costituita dal valore hash per ogni file dei risultati della query separato da uno spazio. Il file di firma elenca la `fileHashValue` per ogni file dei risultati della query.

Fasi di implementazione della convalida personalizzata

Durante l'implementazione di una soluzione di convalida personalizzata, è necessario convalidare il file di firma per primo e, succesisvamente, i file dei risultati della query a cui fa riferimento.

Convalida del file di firma

Per convalidare un file di firma, è necessario disporre della relativa firma, della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file e di una stringa di firma dei dati che si elaborerà personalmente.

1. Ottenere il file di firma.
2. Verificare che il file di firma sia stato recuperato dal relativo percorso originale.
3. Recuperare la firma con codifica esadecimale del file di firma.
4. Recuperare l'impronta con codifica esadecimale della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file di firma.
5. Recuperare la chiave pubblica per l'intervallo di tempo corrispondente a `queryCompleteTime` nel file di firma. Per l'intervallo di tempo, scegliere un intervallo che sia `StartTime` precedente rispetto a `queryCompleteTime` e uno che sia `EndTime` successivo rispetto a `queryCompleteTime`.
6. Tra le chiavi pubbliche recuperate, scegliere la chiave pubblica con l'impronta corrispondente al valore `publicKeyFingerprint` nel file di firma.
7. Utilizzando un elenco hash contenente il valore hash per ogni file dei risultati della query separato da uno spazio, ricreare la stringa di firma dei dati utilizzata per verificare la firma del file di firma. Il file di firma elenca la `fileHashValue` per ogni file dei risultati della query.

   Ad esempio, se l'array `files` del proprio file di firma contiene i seguenti tre file di risultati della query, la lista hash è "aaa bbb ccc".

   ```
   “files": [

      {

           "fileHashValue" : “aaa”,
   ```

```
        "fileName" : "result_1.csv.gz"

    },
    {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

    },
    {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

    }
],
```

8. Per convalidare la firma, passare l'hash SHA-256 della stringa, la chiave pubblica e la firma come parametri all'algoritmo RSA di verifica della firma. Se il risultato è true, il file di firma è valido.

Convalida dei file dei risultati della query

Se il file di firma è valido, convalidare i file dei risultati della query a cui fa riferimento il file di firma. Per convalidare l'integrità di un file dei risultati della query, calcolare il relativo valore hash SHA-256 sul contenuto compresso e confrontare i risultati con il `fileHashValue` per il file dei risultati della query registrato nel file di firma. Se i valori hash corrispondono, il file dei risultati della query è valido.

Le seguenti sezioni descrivono in dettaglio la procedura di convalida.

A. Ottenere il file di firma

I primi passaggi sono ottenere il file di firma e ottenere l'impronta digitale della chiave pubblica.

1. Scaricare il file di firma dal proprio bucket Amazon S3 per i risultati della query che si desidera convalidare.
2. Quindi, recuperare il valore `hashSignature` dal file di firma.
3. Nel file di firma recuperare l'impronta della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file di firma dal campo `publicKeyFingerprint`.

B. Recupero della chiave pubblica per la convalida del file di firma

Per ottenere la chiave pubblica per convalidare il file di firma, puoi utilizzare l' AWS CLI o l' CloudTrail API. In entrambi i casi, è possibile specificare un intervallo di tempo (ovvero un'ora di inizio e una di fine) per il file di firma da convalidare. Utilizzare un intervallo di tempo corrispondente a quello `queryCompleteTime` indicato nel file di firma. È possibile che vengano restituite una o più chiavi pubbliche per l'intervallo di tempo specificato. Le chiavi restituite possono avere intervalli di tempo di validità sovrapposti.

> **Note**
>
> Poiché CloudTrail utilizza coppie di private/public chiavi diverse per regione, ogni file di firma è firmato con una chiave privata unica per la regione. Pertanto, quando si convalida un file di firma da una determinata Regione, è necessario recuperare la relativa chiave pubblica dalla stessa Regione.

Usa il AWS CLI per recuperare le chiavi pubbliche

Per recuperare una chiave pubblica per un file di firma utilizzando il AWS CLI, usa il `cloudtrail list-public-keys` comando. Il comando ha il formato seguente:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time
<end-time>]
```

I parametri relativi all'ora di inizio e all'ora di fine sono time stamp UTC facoltativi. Se non specificata, verrà utilizzata l'ora corrente e verranno restituite la chiave o le chiavi pubbliche attualmente attive.

Risposta di esempio

La risposta sarà un elenco di oggetti JSON che rappresentano la chiave o le chiavi restituite:

Utilizza l' CloudTrail API per recuperare le chiavi pubbliche

Per recuperare una chiave pubblica per un file di firma utilizzando l' CloudTrail API, trasmetti i valori dell'ora di inizio e dell'ora di fine all'`ListPublicKeys`API. L'API `ListPublicKeys` restituisce le chiavi pubbliche le cui chiavi private sono state utilizzate per firmare il file di firma compresi nell'intervallo di tempo specificato. Per ogni chiave pubblica, l'API restituisce anche le corrispondenti impronte.

`ListPublicKeys`

Questa sezione descrive i parametri di richiesta e gli elementi di risposta dell'API `ListPublicKeys`.

> **Note**
>
> La codifica dei campi binari per `ListPublicKeys` è soggetta a modifiche.

Parametri della richiesta

Nome	Descrizione
`StartTime`	Facoltativamente, specifica, in UTC, l'inizio dell'intervallo di tempo in cui cercare la chiave pubblica per il file di firma. CloudTrail Se non StartTime è specificato, viene utilizzata l'ora corrente e viene restituita la chiave pubblica corrente. Tipo: DateTime
`EndTime`	Facoltativamente, specifica, in UTC, la fine dell'intervallo di tempo in cui cercare le chiavi pubbliche per CloudTrail i file di firma. Se non EndTime è specificato, viene utilizzata l'ora corrente. Tipo: DateTime

Elementi di risposta

`PublicKeyList`, una matrice di oggetti `PublicKey` contenenti:

Nome	Descrizione
`Value`	Valore della chiave pubblica con codifica DER in formato PKCS #1. Tipo: Blob
`ValidityStartTime`	Ora di inizio della validità della chiave pubblica. Tipo: DateTime

`ValidityEndTime`	Ora di fine della validità della chiave pubblica. Tipo: DateTime
`Fingerprint`	Impronta della chiave pubblica. L'impronta può essere utilizzata per identificare la chiave pubblica da utilizzare per convalidare il file di firma. Tipo: stringa

C. Scelta della chiave pubblica da utilizzare per la convalida

Tra le chiavi pubbliche recuperate da `list-public-keys` o `ListPublicKeys`, scegliere la chiave pubblica la cui impronta corrisponde all'impronta registrata nel campo `publicKeyFingerprint` del file di firma. Questa è la chiave pubblica che verrà utilizzata per convalidare il file di firma.

D. Creazione di una nuova stringa di firma dei dati

Ora che si dispone della firma del file di firma e della chiave pubblica associata, occore calcolare la stringa di firma dei dati. Dopo aver calcolato tale stringa, si disporrà di tutte le informazioni necessarie per verificare la firma.

La stringa di firma dei dati è costituita dal valore hash per ogni file dei risultati della query separato da uno spazio. Dopo aver ricreato questa stringa, sarà possibile convalidare il file di firma.

E. Convalida del file di firma

A questo punto è possibile passare la stringa di firma dei dati ricreata, la firma digitale e la chiave pubblica all'algoritmo RSA di verifica della firma. Se l'output è true, la firma del file di firma è verificata e il file di firma è valido.

F. Convalida dei file dei risultati della query

Dopo aver convalidato il file di firma, è possibile convalidare il file dei risultati della query a cui fa riferimento. Il file di firma contiene gli hash SHA-256 dei file dei risultati della query. Se uno dei file dei risultati della query è stato modificato dopo la CloudTrail consegna, gli hash SHA-256 cambieranno e la firma del file di firma non corrisponderà.

Utilizzare la procedura seguente per convalidare i file dei risultati della query elencati nell'array `files` del file di firma.

1. Recuperare il valore hash originale del file dal campo `files.fileHashValue` all'interno del file di firma.
2. Eseguire l'hashing dei contenuti compressi del file dei risultati della query con l'algoritmo di hashing specificato in `hashAlgorithm`.
3. Confrontare il valore hash generato per ogni file dei risultati della query con il `files.fileHashValue` nel file di firma. Se gli hash corrispondono, i file dei risultati della query sono validi.

Convalida offline dei file di firma e dei risultati della query

Durante la convalida offline dei file di firma e dei risultati della query, in genere è possibile fare riferimento alle procedure descritte nelle sezioni precedenti. Tuttavia, è necessario tenere conto delle seguenti informazioni sulle chiavi pubbliche.

Chiavi pubbliche

Per eseguire la convalida offline, la chiave pubblica necessaria per convalidare i file dei risultati della query in un determinato intervallo di tempo deve prima essere recuperata online (chiamando `ListPublicKeys`, ad esempio) e quindi memorizzata in modo sicuro offline. Questo passaggio deve essere ripetuto ogni volta che si vuole convalidare altri file non compresi nell'intervallo di tempo iniziale specificato.

Esempio di frammento di codice di convalida

Il seguente frammento di esempio fornisce un codice scheletrico per la convalida CloudTrail dei file dei risultati delle query e dei segni. Lo skeleton code è online/offline agnostico, ovvero sta all'utente decidere se implementarlo con o senza connettività online a. AWS L'implementazione suggerita usa i provider di sicurezza Java Cryptography Extension (JCE) e Bouncy Castle.

Il frammento di codice di esempio mostra:

- Come creare la stringa di firma dei dati utilizzata per convalidare la firma del file di firma.
- Come verificare la firma del file di firma.
- Come calcolare il valore hash per il file dei risultati della query e confrontarlo con il `fileHashValue` elencato nel file di firma per verificare l'autenticità del file dei risultati della query.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
```

```
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
 file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
 copy
```

```
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }

            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
```

```
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
 AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
 rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

Ottimizza le query su Lake CloudTrail

Questa pagina fornisce indicazioni su come ottimizzare le query CloudTrail Lake per migliorare le prestazioni e l'affidabilità. Descrive tecniche di ottimizzazione specifiche e soluzioni alternative per gli errori di query più comuni.

Argomenti

- Consigli per l'ottimizzazione delle interrogazioni
- Soluzioni alternative per gli errori di interrogazione

Consigli per l'ottimizzazione delle interrogazioni

Segui i consigli in questa sezione per ottimizzare le tue query.

Raccomandazioni:

- Ottimizza le aggregazioni
- Utilizzate tecniche di approssimazione
- Limita i risultati delle interrogazioni
- Ottimizza le query LIKE
- Usa invece di UNION ALLUNION
- Come includere solo le colonne obbligatorie
- Riduci l'ambito della funzione della finestra

Ottimizza le aggregazioni

L'esclusione di colonne ridondanti nelle `GROUP BY` clausole può migliorare le prestazioni poiché un numero inferiore di colonne richiede meno memoria. Ad esempio, nella seguente query, possiamo usare la `arbitrary` funzione su una colonna ridondante per migliorare le prestazioni. `eventType` La `arbitrary` funzione on `eventType` viene utilizzata per selezionare il valore del campo in modo casuale dal gruppo poiché il valore è lo stesso e non deve essere incluso nella clausola. `GROUP BY`

```
SELECT eventName, eventSource, arbitrary(eventType), count(*)
FROM $EDS_ID
GROUP BY eventName, eventSource
```

È possibile migliorare le prestazioni della `GROUP BY` funzione ordinando l'elenco dei campi all'interno dell'ordine decrescente del loro numero di valori univoci (cardinalità). `GROUP BY` Ad esempio, oltre a calcolare il numero di eventi di un tipo in ciascuno di essi Regione AWS, è possibile migliorare le prestazioni utilizzando`eventName`, `awsRegion` order in the `GROUP BY` function anzichè`awsRegion`, `eventName` poiché i valori univoci di sono più numerosi di `eventName` quelli esistenti. `awsRegion`

```
SELECT eventName, awsRegion, count(*)
FROM $EDS_ID
GROUP BY eventName, awsRegion
```

Utilizzate tecniche di approssimazione

Ogni volta che non sono necessari valori esatti per contare valori distinti, utilizza funzioni di aggregazione approssimative per trovare i valori più frequenti. Ad esempio, `approx_distinct`utilizza molta meno memoria e viene eseguito più velocemente dell'operazione. `COUNT(DISTINCT fieldName)`

Limita i risultati delle interrogazioni

Se è necessaria solo una risposta di esempio per una query, limita i risultati a un numero limitato di righe utilizzando la `LIMIT` condizione. In caso contrario, la query restituirà risultati di grandi dimensioni e richiederà più tempo per l'esecuzione della query.

L'utilizzo di `LIMIT` along with `ORDER BY` consente di ottenere risultati più rapidamente per i primi o gli ultimi N record, in quanto riduce la quantità di memoria necessaria e il tempo necessario per l'ordinamento.

```
SELECT * FROM $EDS_ID
ORDER BY eventTime
LIMIT 100;
```

Ottimizza le query LIKE

Puoi usare `LIKE` per trovare stringhe corrispondenti, ma per le stringhe lunghe richiede molto calcolo. La `regexp_like`funzione è nella maggior parte dei casi un'alternativa più veloce.

Spesso è possibile ottimizzare una ricerca ancorando la sottostringa che si sta cercando. Ad esempio, se stai cercando un prefisso, è meglio usare '`substr`%' invece di '% `substr` %' con l'`LIKE`operatore e '^' con la funzione. `substr` `regexp_like`

Usa invece di **`UNION ALL`**`UNION`

`UNION ALL`e `UNION` sono due modi per combinare i risultati di due interrogazioni in un unico risultato, ma `UNION` rimuovono i duplicati. `UNION`deve elaborare tutti i record e trovare i duplicati, operazione che richiede molta memoria e calcolo, ma `UNION ALL` è un'operazione relativamente rapida. A meno che non sia necessario deduplicare i record, utilizza `UNION ALL` per ottenere prestazioni ottimali.

Come includere solo le colonne obbligatorie

Se non hai bisogno di una colonna, non includerla nella query. Minore è la quantità di dati che una query deve elaborare, maggiore sarà la velocità di esecuzione. Se hai interrogazioni che riguardano la query più esterna, dovresti modificarla `SELECT *` in un elenco di colonne di cui hai bisogno. *

La clausola `ORDER BY` restituisce i risultati di una query disponendoli in ordine. Quando si ordinano grandi quantità di dati, se la memoria richiesta non è disponibile, i risultati ordinati intermedi vengono scritti su disco, il che può rallentare l'esecuzione delle query. Se non è strettamente necessario

ordinare i risultati, evita di aggiungere una clausola `ORDER BY`. Inoltre, evitate di aggiungere `ORDER BY` elementi alle interrogazioni interne se non sono strettamente necessari.

Riduci l'ambito della funzione della finestra

Le funzioni della finestra mantengono in memoria tutti i record su cui operano per calcolarne il risultato. Quando la finestra è di dimensioni molto grandi, la funzione finestra può esaurire la memoria. Per assicurarvi che le interrogazioni vengano eseguite entro i limiti di memoria disponibili, riducete le dimensioni delle finestre su cui operano le funzioni della finestra aggiungendo una `PARTITION BY` clausola.

A volte le query con le funzioni finestra possono essere riscritte senza funzioni finestra. Ad esempio, invece di utilizzare `row_number` or`rank`, puoi utilizzare funzioni aggregate come o. `max_bymin_by`

La seguente query trova l'alias assegnato più di recente a ciascuna chiave KMS utilizzando. `max_by`

```
SELECT element_at(requestParameters, 'targetKeyId') as keyId,
max_by(element_at(requestParameters, 'aliasName'), eventTime) as mostRecentAlias
FROM $EDS_ID
WHERE eventsource = 'kms.amazonaws.com'
AND eventName in ('CreateAlias', 'UpdateAlias')
AND eventTime > DATE_ADD('week', -1, CURRENT_TIMESTAMP)
GROUP BY element_at(requestParameters, 'targetKeyId')
```

In questo caso, la `max_by` funzione restituisce l'alias per il record con l'ora dell'ultimo evento all'interno del gruppo. Questa query viene eseguita più velocemente e utilizza meno memoria rispetto a una query equivalente con una funzione finestra.

Soluzioni alternative per gli errori di interrogazione

Questa sezione fornisce soluzioni alternative per gli errori di query più comuni.

Errori di interrogazione:

- La query fallisce perché la risposta è troppo grande
- La query ha esito negativo a causa dell'esaurimento delle risorse

La query fallisce perché la risposta è troppo grande

Una query può avere esito negativo se la risposta risultante nel messaggio è troppo grande**`Query response is too large`**. In tal caso, è possibile ridurre l'ambito di aggregazione.

Funzioni di aggregazione come quelle che `array_agg` possono far sì che almeno una riga nella risposta alla query sia molto grande, causando l'esito negativo della query. Ad esempio, l'utilizzo di `array_agg(eventName)` instead of `array_agg(DISTINCT eventName)` aumenterà notevolmente la dimensione della risposta a causa della duplicazione dei nomi degli eventi selezionati CloudTrail .

La query ha esito negativo a causa dell'esaurimento delle risorse

Se non è disponibile memoria sufficiente durante l'esecuzione di operazioni a uso intensivo di memoria come join, aggregazioni e funzioni delle finestre, i risultati intermedi vengono trasferiti su disco, ma la fuoriuscita rallenta l'esecuzione delle query e può essere insufficiente per evitare che la query abbia esito negativo. **`Query exhausted resources at this scale factor`** Questo problema può essere risolto riprovando l'interrogazione.

Se gli errori di cui sopra persistono anche dopo l'ottimizzazione della query, è possibile ridimensionare l'ambito `eventTime` della query utilizzando gli eventi ed eseguirla più volte a intervalli più piccoli dell'intervallo di tempo della query originale.

Esegui e gestisci le query di CloudTrail Lake con AWS CLI

Puoi usare il AWS CLI per eseguire e gestire le tue query CloudTrail Lake. Quando usi il AWS CLI, ricorda che i tuoi comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Comandi disponibili per le query su CloudTrail Lake

I comandi per l'esecuzione e la gestione delle query in CloudTrail Lake includono:

- `start-query`per eseguire una query.
- `describe-query`per restituire i metadati relativi a una query.
- `generate-query`per produrre una query da un prompt in lingua inglese. Per ulteriori informazioni, consulta Crea query su CloudTrail Lake da istruzioni in linguaggio naturale.
- `get-query-results`per restituire i risultati della query per l'ID di query specificato.
- `list-queries`per ottenere un elenco di interrogazioni per il data store degli eventi specificato.
- `cancel-query`per annullare una query in esecuzione.

Per un elenco dei comandi disponibili per i data store di eventi CloudTrail Lake, vediComandi disponibili per gli archivi dati degli eventi.

Per un elenco dei comandi disponibili per le dashboard di CloudTrail Lake, consultaComandi disponibili per i dashboard.

Per un elenco dei comandi disponibili per le integrazioni di CloudTrail Lake, consulta. Comandi disponibili per le integrazioni con CloudTrail Lake

Produci una query da un prompt in linguaggio naturale con AWS CLI

Esegui il `generate-query` comando per generare una query da un prompt in inglese. Per`--event-data-stores`, fornisci l'ARN (o il suffisso ID dell'ARN) dell'archivio dati degli eventi su cui desideri eseguire la query. È possibile specificare un solo archivio dati di eventi. Per`--prompt`, fornisci il prompt in inglese.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

In caso di successo, il comando genera un'istruzione SQL e ne fornisce un'istruzione `QueryAlias` che verrà utilizzata con il `start-query` comando per eseguire la query sull'archivio dati degli eventi.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

Avviare una query con AWS CLI

Il AWS CLI start-query comando di esempio seguente esegue una query sull'event data store specificato come ID nell'istruzione di query e consegna i risultati della query a un bucket S3 specificato. Il parametro `--query-statement` obbligatorio fornisce una query SQL racchiusa tra virgolette singole. I parametri opzionali includono `--delivery-s3-uri`, per fornire i risultati della query a un bucket S3 specificato. Per ulteriori informazioni sul linguaggio di interrogazione che puoi usare in CloudTrail Lake, consulta. CloudTrail Vincoli Lake SQL

```
aws cloudtrail start-query
```

```
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3-uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

La risposta è una stringa `QueryId`. Per ottenere lo stato di una query, eseguire describe-query utilizzando il valore `QueryId` restituito da start-query. Se la query ha esito positivo, è possibile eseguire get-query-results per ottenere i risultati.

Output

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Le query che vengono eseguite per più di un'ora potrebbero scadere. È comunque possibile ottenere risultati parziali elaborati prima del timeout della query.
> Se stai inviando i risultati della query a un bucket S3 utilizzando il `--delivery-s3-uri` parametro opzionale, la policy del bucket deve concedere l' CloudTrailautorizzazione a recapitare i risultati della query al bucket. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake.

Ottieni i metadati relativi a una query con AWS CLI

Il AWS CLI describe-query comando di esempio seguente ottiene i metadati relativi a una query, tra cui il tempo di esecuzione della query in millisecondi, il numero di eventi analizzati e corrispondenti, il numero totale di byte analizzati e lo stato della query. Il valore `BytesScanned` corrisponde al numero di byte per i quali viene fatturato l'account per la query, a meno che la query non sia ancora in esecuzione. Se i risultati della query sono stati inviati a un bucket S3, la risposta fornirà anche l'URI S3 e lo stato di consegna.

Puoi specificare un valore per il parametro `--query-id` o `--query-alias`. La specifica del parametro `--query-alias` restituisce informazioni sull'ultima query eseguita per l'alias.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Di seguito è riportata una risposta di esempio.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

Ottieni i risultati delle query con AWS CLI

Il comando di esempio seguente della AWS CLI get-query-results ottiene i risultati dei dati degli eventi di una query. È necessario specificare il `--query-id` restituito dal comando start-query. Il valore `BytesScanned` corrisponde al numero di byte per i quali viene fatturato l'account per la query, a meno che la query non sia ancora in esecuzione. I parametri opzionali includono `--max-query-results`, che consente di specificare il numero massimo di risultati che desideri che il comando restituisca su una singola pagina. Se ci sono più risultati di quanto specificato dal valore `--max-query-results`, esegui nuovamente il comando aggiungendo il valore `NextToken` restituito per visualizzare la pagina dei risultati successiva.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Output

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
```

```
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

Elenca tutte le query su un archivio dati di eventi con AWS CLI

Il comando di esempio seguente della AWS CLI list-queries restituisce un elenco delle query e dei relativi stati eseguite su un archivio di dati degli eventi specificato negli ultimi sette giorni. È necessario specificare un valore di ARN o di suffisso ID di un ARN per `--event-data-store`. Facoltativamente, per restringere l'elenco dei risultati, è possibile specificare un intervallo di tempo, formattato come marche temporali, aggiungendo i parametri `--start-time` e `--end-time` e un valore `--query-status`. I valori validi per `QueryStatus` includono: `QUEUED`, `RUNNING`, `FINISHED`, `FAILED` o `CANCELLED`.

list-queries ha anche parametri di impaginazione opzionali. Utilizza `--max-results` per specificare il numero massimo di risultati che desideri che il comando restituisca su una singola pagina. Se ci sono più risultati di quanto specificato dal valore `--max-results`, esegui nuovamente il comando aggiungendo il valore `NextToken` restituito per visualizzare la pagina dei risultati successiva.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

Output

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
```

```
            "QueryStatus": "CANCELLED",
            "CreationTime": 1598296624
        }
    ],
    "NextToken": "20add42078135EXAMPLE"
}
```

Annullare una query in esecuzione con AWS CLI

Il AWS CLI cancel-query comando di esempio seguente annulla una query con lo stato di`RUNNING`. Devi specificare un valore per `--query-id`. Quando esegui cancel-query, lo stato della query potrebbe essere visualizzato come `CANCELLED` anche se l'operazione cancel-query non è ancora terminata.

> **Note**
>
> Una query annullata può comportare addebiti. Sul proprio account sarà comunque addebitata la quantità di dati che è stata scansionata prima dell'annullamento della query.

Di seguito è riportato un esempio della CLI.

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Output

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail Vincoli Lake SQL

CloudTrail Le query Lake sono stringhe SQL. Questa sezione contiene informazioni relative alle funzioni, agli operatori e agli schemi supportati.

Sono consentite soltanto istruzioni `SELECT`. Nessuna stringa di query può modificare o alterare i dati.

La sintassi CloudTrail Lake per un'`SELECT`istruzione è la seguente. L'ID del data store degli eventi, la parte ID dell'ARN dell'Event Data Store, è specificato per il valore. `FROM`

```
SELECT [ DISTINCT ] columns [ Aggregate ]
[ FROM table event_data_store_ID]
[ WHERE columns [ Conditions ] ]
[ GROUP BY columns [ DISTINCT | Aggregate ] ]
[ HAVING columns [ Aggregate | Conditions ] ]
[ ORDER BY columns [ Aggregate | ASC | DESC | NULLS | FIRST | LAST ]
[ LIMIT [ INT ] ]
```

CloudTrail Lake supporta tutte le istruzioni, le funzioni e gli operatori Trino `SELECT` SQL validi. Per ulteriori informazioni sulle funzioni e gli operatori SQL supportati, consulta Funzioni e operatori sul sito Web della documentazione di Trino.

La CloudTrail console fornisce una serie di query di esempio che possono aiutarti a iniziare a scrivere le tue query. Per ulteriori informazioni, consulta Visualizza query di esempio con la console CloudTrail .

Per informazioni su come ottimizzare le query, consulta. Ottimizza le query su Lake CloudTrail

Argomenti

- Funzioni, condizioni e operatori join supportati
- Supporto avanzato per query multi-tabella

Funzioni, condizioni e operatori join supportati

Funzioni supportate

CloudTrail Lake supporta tutte le funzioni di Trino. Per ulteriori informazioni sulle funzioni supportate, consulta Funzioni e operatori sul sito web della documentazione di Trino.

Operatori di condizioni supportati

Di seguito sono riportati gli operatori di condizione supportati.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
```

```
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

Operatori join supportati

Sono supportati i seguenti operatori `JOIN`: Per ulteriori informazioni sull'esecuzione di query multi-tabella, consulta Supporto avanzato per query multi-tabella.

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

Supporto avanzato per query multi-tabella

CloudTrail Lake supporta un linguaggio di interrogazione avanzato su più archivi di dati di eventi.

- `UNION|UNION ALL|EXCEPT|INTERSECT`
- `LEFT|RIGHT|INNER JOIN`

Per eseguire la query, utilizza il comando start-query nella AWS CLI. Di seguito è riportato un esempio, che utilizza una delle query di esempio in questa sezione.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

La risposta è una stringa `QueryId`. Per ottenere lo stato di una query, esegui `describe-query` utilizzando il valore `QueryId` restituito da `start-query`. Se la query ha esito positivo, è possibile eseguire `get-query-results` per ottenere i risultati.

`UNION|UNION ALL|EXCEPT|INTERSECT`

Di seguito è riportato un esempio di query che utilizza `UNION` e trova gli eventi in base `UNION ALL` all'ID e al nome dell'evento in tre archivi di dati di eventi EDS1, EDS2, e EDS3. I risultati vengono prima selezionati dall'archivio dati di ciascun evento, quindi i risultati vengono concatenati, ordinati per ID evento e limitati a dieci eventi.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

`LEFT|RIGHT|INNER JOIN`

Di seguito è riportata una query di esempio che utilizza `LEFT JOIN` per trovare tutti gli eventi di un datastore di eventi denominato `eds2`, mappato a `edsB`, che corrispondono a quelli in un datastore di eventi primario (a sinistra), `edsA`. Gli eventi restituiti si verificano entro il 1° gennaio 2020 compreso e vengono restituiti solo i nomi degli eventi.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

Schemi SQL supportati per datastore di eventi

Le seguenti sezioni forniscono lo schema SQL supportato per ogni tipo di datastore di eventi.

Argomenti

- Schema supportato per i campi di registrazione CloudTrail degli eventi
- Schema supportato per i campi di registrazione degli eventi di CloudTrail Insights

- Schema supportato per i campi dei record degli elementi di configurazione AWS Config
- Schema supportato per i campi di registrazione delle prove AWS Audit Manager
- Schema supportato per i campi non associati agli eventi AWS

Schema supportato per i campi di registrazione CloudTrail degli eventi

Di seguito è riportato lo schema SQL valido per i campi di registrazione degli eventi di CloudTrail gestione, dati e attività di rete. Per ulteriori informazioni sui campi di registrazione CloudTrail degli eventi, vedereCloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
 "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

 username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

 mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

 accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

 attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,

 ec2issuedinvpc:string>,onbehalfof:struct<userid:string,identitystorearn:string>,

 inscopeof:struct<sourcearn:string,sourceaccount:string,issuertype:string,
                 credentiaisissuedto:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
```

```
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
```

```
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "vpcendpointaccountid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
```

```
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

Schema supportato per i campi di registrazione degli eventi di CloudTrail Insights

Di seguito è riportato lo schema SQL valido per i campi dei registri degli eventi Insights.
Per gli eventi Insights, il valore di `eventcategory` è `Insight` e il valore di `eventtype` è

`AwsCloudTrailInsight`. Per le descrizioni di questi campi, vedereCloudTrail registra i contenuti per gli eventi Insights per i datastore di eventi Lake..

> **Note**
>
> I `baselineaverage` campi `insightvalueinsightaverage`,`baselinevalue`, e all'interno del `attributions` campo di `insightContext` inizieranno a essere obsoleti il 23 giugno 2025.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
```

```
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type": "struct<baselineaverage:double,insightaverage:double,
                 baselineduration:integer,insightduration:integer,
                 attributions:struct<attribute:string,insightvalue:string,
                 insightaverage:double,baselinevalue:string,baselineaverage:double,
                 insight:struct<value:string,average:double>,
                 baseline:struct<value:string,average:double>>>"
    }
]
```

Schema supportato per i campi dei record degli elementi di configurazione AWS Config

Di seguito è riportato lo schema SQL valido per i campi dei registri degli elementi di configurazione. Per gli elementi di configurazione, il valore di `eventcategory` è `ConfigurationItem` e il valore di `eventtype` è `AwsConfigurationItem`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:
```

```
 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

Schema supportato per i campi di registrazione delle prove AWS Audit Manager

Di seguito è riportato lo schema SQL valido per i campi dei registri delle prove Audit Manager. Per i campi dei record di prova di Audit Manager, il valore di `eventcategory` è `Evidence` e il valore di `eventtype` è `AwsAuditManagerEvidence`. Per ulteriori informazioni sull'aggregazione delle prove in CloudTrail Lake utilizzando Audit Manager, consulta Evidence finder nella Guida per l'AWS Audit Manager utente.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
```

```
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                 evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

Schema supportato per i campi non associati agli eventi AWS

Di seguito è riportato lo schema SQL valido per AWS gli eventi diversi. Per i non AWS eventi, il valore di `eventcategory` è `ActivityAuditLog` e il valore di `eventtype` è`ActivityLog`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
```

```
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                 recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

CloudWatch Metriche supportate

CloudTrail Lake supporta le CloudWatch metriche di Amazon. CloudWatch è un servizio di monitoraggio delle AWS risorse. È possibile CloudWatch utilizzarlo per raccogliere e tenere traccia delle metriche, impostare allarmi e reagire automaticamente ai cambiamenti nelle risorse. AWS

Il `AWS/CloudTrail` namespace include le seguenti metriche per Lake. CloudTrail

Parametro	Descrizione	unità
`HourlyDataIngested`	La quantità di dati importati nelil datastore di eventi durante l'ultima ora. Questa metrica viene aggiornata ogni ora. Questa metrica è disponibile per tutti i tipi di datastore di eventi.	Byte
`TotalDataRetained`	La quantità di dati mantenuti nelil datastore di eventi durante l'intero periodo di conservazione. Questa metrica viene aggiornata ogni notte. Questa metrica è disponibile per tutti i tipi di datastore di eventi.	Byte
`TotalStorageBytes`	Il totale dei byte compressi nel datastore di eventi al giorno corrente. Questa metrica è disponibile per tutti i tipi di datastore di eventi.	Byte

Parametro	Descrizione	unità
`TotalPaidStorageBytes`	Per i datastore di eventi che utilizzano l'opzione di prezzo per la conservazione estendibile di un anno, si tratta del totale di byte compressi dopo 366 giorni fino al periodo di conservazione massimo configurato per il datastore di eventi. Per i datastore di eventi che utilizzano l'opzione di prezzo per la conservazione estendibile di un anno, l'archiviazione è inclusa nel prezzo di importazione senza costi aggiuntivi per i primi 366 giorni, ossia il periodo di conservazione predefinito per il datastore di eventi. Dopo 366 giorni, lo spazio di archiviazione è. pay-as-you-go Per informazioni sui prezzi, consulta Prezzi di AWS CloudTrail. Questa metrica è disponibile solo per i datastore di eventi che utilizzano l'opzione di prezzo per la conservazione estendibile di un anno.	Byte

Parametro	Descrizione	unità
`HourlyEventsAnalyzed`	Il numero totale di eventi analizzati da CloudTrail Insights nell'archivio dati degli eventi. Questa metrica viene aggiornata ogni ora. Questa metrica si riferisce agli archivi di dati di CloudTrail eventi che abilitano CloudTrail Insights.	Conteggio

Per ulteriori informazioni sulle CloudWatch metriche, consulta i seguenti argomenti.

- Utilizzo dei CloudWatch parametri di Amazon
- Utilizzo degli CloudWatch allarmi Amazon

Lavorare con i CloudTrail sentieri

I trail registrano AWS le attività, distribuiscono e archiviano questi eventi in un bucket Amazon S3, con consegna opzionale a CloudWatch Logs e Amazon. EventBridge

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

Puoi creare percorsi multiregionali e a regione singola per i tuoi. Account AWS

Percorsi multiregionali

Quando crei un percorso multiregionale, CloudTrail registra gli eventi in tutto ciò Regioni AWS che è abilitato nel tuo Account AWS e invia i file di registro degli CloudTrail eventi a un bucket S3 da te specificato. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multiregionali. È possibile convertire un percorso a regione singola in un percorso multiregionale utilizzando. AWS CLI Per ulteriori informazioni, consulta Comprendere i percorsi multiregionali e le regioni opt-in, Creazione di un percorso con la console e Conversione di un percorso a regione singola in un percorso multiregionale.

Percorsi a regione singola

Quando crei un percorso a regione singola, CloudTrail registra solo gli eventi in quella regione. Quindi invia i file di registro CloudTrail degli eventi a un bucket Amazon S3 specificato dall'utente. Puoi creare un percorso basato su una singola Regione solo utilizzando la AWS CLI. Se crei percorsi singoli aggiuntivi, puoi fare in modo che questi percorsi consegnino i file di registro CloudTrail degli eventi nello stesso bucket S3 o in bucket separati. Questa è l'opzione predefinita quando crei un trail utilizzando AWS CLI o l'API. CloudTrail Per ulteriori informazioni, consulta Creazione, aggiornamento e gestione di percorsi con AWS CLI.

> **Note**
>
> Per entrambi i tipi di percorsi, puoi specificare un bucket Amazon S3 di qualsiasi Regione.

Se hai creato un'organizzazione in AWS Organizations, puoi creare un percorso organizzativo che registri tutti gli eventi per tutti gli AWS account di quell'organizzazione. Gli itinerari organizzativi possono essere applicati a tutte le AWS regioni o alla regione corrente. I percorsi dell'organizzazione devono essere creati nell'account di gestione o nell'account dell'amministratore delegato e, se specificati come applicabili a un'organizzazione, vengono applicati automaticamente a tutti gli account membri dell'organizzazione. Gli account dei membri possono visualizzare il percorso dell'organizzazione, ma non possono modificarlo o eliminarlo. Per impostazione predefinita, gli account membro non hanno accesso ai file di log del trail dell'organizzazione nel bucket Amazon S3. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione.

Argomenti

- Creare un percorso per il tuo Account AWS
- Creazione di un percorso per un'organizzazione
- Comprendere i percorsi multiregionali e le regioni opt-in
- Copiare gli eventi del percorso su CloudTrail Lake
- Acquisizione e visualizzazione dei file di CloudTrail registro
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Utilizzo AWS CloudTrail con gli endpoint VPC dell'interfaccia
- Requisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS
- Account AWS chiusura e percorsi

Creare un percorso per il tuo Account AWS

Quando crei un percorso, abiliti la distribuzione continua di eventi come file di log su un bucket Amazon S3 specificato. La creazione di un trail offre molti vantaggi, tra cui:

- Un record di eventi che si estende per oltre 90 giorni.
- L'opzione per monitorare e inviare avvisi automaticamente su eventi specifici inviando eventi di registro ad Amazon CloudWatch Logs.
- L'opzione per interrogare i log e analizzare l'attività AWS del servizio con Amazon Athena.

A partire dal 12 aprile 2019, puoi visualizzare i percorsi solo AWS nelle regioni in cui registrano gli eventi. Se crei un percorso multiregionale, questo viene visualizzato nella console in tutte Regioni AWS le aree abilitate nel tuo account. Se crei un percorso che registra eventi in una sola regione ,

puoi visualizzarlo e gestirlo solo in quella regione . Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multiregionali. Per creare un percorso a singola Regione, devi utilizzare la AWS CLI.

Se lo utilizzi AWS Organizations, puoi creare un percorso che registrerà gli eventi per tutti gli AWS account dell'organizzazione. Un percorso con lo stesso nome verrà creato in ogni account membro e gli eventi di ogni percorso verranno distribuiti nel bucket Amazon S3 specificato.

> **Note**
>
> Solo l'account di gestione o l'account dell'amministratore delegato per un'organizzazione possono creare un trail per l'organizzazione. La creazione di un percorso per un'organizzazione abilita automaticamente l'integrazione tra CloudTrail e Organizations. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione.
> Se configuri male il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterà di recapitare i file di registro al bucket S3 per 30 giorni e questi attempted-to-deliver eventi saranno soggetti alle tariffe standard. CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Argomenti

- Creazione e aggiornamento di un percorso con la console
- Creazione, aggiornamento e gestione di percorsi con AWS CLI
- Creazione di percorsi multipli

Creazione e aggiornamento di un percorso con la console

Puoi usare la CloudTrail console per creare, aggiornare o eliminare i tuoi percorsi. I percorsi creati utilizzando la console sono multi-regione. Per creare un percorso che registri gli eventi in uno solo Regione AWS, usa il AWS CLI.

Puoi creare fino a cinque percorsi per ogni Regione. Dopo aver creato un percorso, inizia CloudTrail automaticamente a registrare le chiamate API e gli eventi correlati nel tuo account nel bucket Amazon S3 da te specificato.

Puoi modificare le seguenti impostazioni per il tuo percorso utilizzando la console: CloudTrail

- Puoi modificare la posizione del bucket S3 e specificare un prefisso.
- L'account di gestione di un' AWS Organizations organizzazione può convertire un itinerario a livello di account in un percorso organizzativo oppure può convertire un itinerario dell'organizzazione in un itinerario a livello di account.
- È possibile abilitare o disabilitare la crittografia delle chiavi KMS.
- È possibile abilitare o disabilitare la convalida dei file di registro. La convalida dei file di registro consente di determinare se un file di registro è stato modificato, eliminato o è rimasto invariato dopo la CloudTrail consegna. Per impostazione predefinita, la convalida dei file di registro è abilitata.
- Puoi configurare un percorso per inviare notifiche a un argomento di Amazon SNS.
- Puoi configurare un percorso per inviare eventi a un gruppo di log di CloudWatch Logs. Sia il gruppo di log che il ruolo IAM devono esistere nel tuo account.
- È possibile aggiornare le impostazioni per eventi di gestione, eventi relativi ai dati, eventi di attività di rete ed eventi Insights.
- È possibile aggiungere o rimuovere tag. Puoi aggiungere fino a 50 coppie di chiavi di tag per aiutarti a identificare i tuoi percorsi.

L'utilizzo della CloudTrail console per creare o aggiornare un percorso offre i seguenti vantaggi.

- Se è la prima volta che si crea un percorso, l'utilizzo della CloudTrail console consente di visualizzare le funzionalità e le opzioni disponibili.
- Se stai configurando un percorso per registrare gli eventi relativi ai dati, l'utilizzo della CloudTrail console ti consente di visualizzare i tipi di dati disponibili. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.
- Se si sta configurando un percorso per gli eventi di attività di rete, l'utilizzo della CloudTrail console consente di visualizzare le fonti di eventi disponibili. Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.

Per informazioni specifiche sulla creazione di un percorso per un'organizzazione in AWS Organizations, vedereCreazione di un percorso per un'organizzazione.

Argomenti

- Creazione di un percorso con la CloudTrail console
- Aggiornamento di un percorso con la CloudTrail console

- Eliminazione di un percorso con la console CloudTrail
- Disattivazione della registrazione per un percorso

Creazione di un percorso con la CloudTrail console

Un percorso può essere applicato a tutto ciò Regioni AWS che è abilitato nella tua Account AWS o può essere applicato a una singola regione. Un percorso che si applica a tutto Regioni AWS ciò che è abilitato nella tua Account AWS viene definito percorso multiregionale. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multi-regione. Puoi creare un percorso basato su una singola Regione solo utilizzando l'operazione AWS CLI o `CreateTrail`API.

> **Note**
>
> Dopo aver creato un percorso, puoi configurare altri Servizi AWS servizi per analizzare e usare i dati evento raccolti nei CloudTrail log. Per ulteriori informazioni, consulta AWS integrazioni di servizi con registri CloudTrail .

Argomenti

- Creazione di un percorso con la console
- Passaggi successivi

Creazione di un percorso con la console

Per creare un percorso multi-regione, utilizza la procedura seguente. Per registrare eventi in una singola Regione (non consigliato), usa la AWS CLI.

Per creare un CloudTrail percorso con AWS Management Console

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nella home page del CloudTrail servizio, nella pagina Percorsi o nella sezione Percorsi della pagina Dashboard, scegli Crea percorso.
3. Nella pagina Create Trail (Crea trail), in Trail name (Nome trail) digitare il nome del trail. Per ulteriori informazioni, consulta Requisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS.

4. Se si tratta di un' AWS Organizations organizzazione, puoi abilitare il percorso per tutti gli account presenti nell'organizzazione. Puoi visualizzare questa opzione solo se hai effettuato l'accesso alla console con un utente o un ruolo nell'account di gestione o nell'account dell'amministratore delegato. Per creare un trail dell'organizzazione, è necessario assicurarsi che l'utente o il ruolo abbiano le autorizzazioni sufficienti. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione.
5. Per Storage location (Posizione di storage), scegli Create new S3 bucket (Crea nuovo bucket S3) per creare un bucket. Quando si crea un bucket, CloudTrail crea e applica le policy bucket obbligatorie. Se scegli di creare un nuovo bucket S3, la tua policy IAM deve includere l'autorizzazione per l'`s3:PutEncryptionConfiguration`azione, perché per impostazione predefinita la crittografia lato server è abilitata per il bucket.

> **Note**
>
> Se scegli Utilizza bucket S3 esistente, specifica un bucket in Nome del bucket del log del percorso oppure scegli Sfoglia per scegliere un bucket. Se desideri utilizzare un bucket in un altro account, devi specificare il nome del bucket. La policy del bucket deve concedere CloudTrail il permesso di scrittura nel bucket stesso. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket Amazon S3 per CloudTrail.

   Per semplificare la ricerca dei registri, creare una nuova cartella (nota anche come prefisso) in un bucket esistente per archiviare i registri. CloudTrail Inserire il prefisso in Prefix (Prefisso).
6. Per Log file SSE-KMS encryption (Crittografia SSE-KMS dei file di log), scegli Enabled (Abilitata) per crittografare i file di log e i file digest utilizzando la crittografia SSE-KMS anziché con SSE-S3. L'impostazione predefinita è Enabled (Abilitata). Se non abiliti la crittografia SSE-KMS, i file di log e i file digest vengono crittografati utilizzando la crittografia SSE-S3. Per ulteriori informazioni sulla crittografia SSE-KMS, consulta Utilizzo della crittografia lato server con (SSE-KMS). AWS Key Management Service Per ulteriori informazioni sulla crittografia SSE-S3, consulta Utilizzo della crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3).

   Se abiliti la crittografia SSE-KMS, scegli Nuova o Esistente. AWS KMS key In AWS KMS Alias (Alias), specificare un alias, nel formato. `alias/` *`MyAliasName`* Per ulteriori informazioni, consultaAggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. CloudTrail supporta anche chiavi AWS KMS multi-regione. Per ulteriori informazioni sulle chiavi multi-

regione, consulta Utilizzo delle chiavi multi-regione nella Guida per gli sviluppatori di AWS Key Management Service .

> **Note**
>
> È anche possibile digitare l'ARN di una chiave da un altro account. Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. La policy della chiave deve CloudTrail permettere di utilizzare la chiave per crittografare i file di log e i file digest e permettere agli utenti specificati di leggere i file di log o i file digest in formato non crittografato. Per informazioni sulla modifica manuale della policy della chiave, consulta Configura le politiche AWS KMS chiave per CloudTrail.

7. In Additional settings (Impostazioni aggiuntive) configura quanto segue.

   a. In Enable log file validation (Abilita la convalida dei file di log), scegli Enabled (Abilitata) per attivare la distribuzione dei file digest di log nel bucket S3. Puoi utilizzare i file digest per verificare che i file di log non siano stati CloudTrail modificati dopo essere stati distribuiti. Per ulteriori informazioni, consulta Convalida dell'integrità dei file di CloudTrail registro.

   b. Per SNS notification delivery (Consegna delle notifiche SNS), scegli Enabled (Abilitata) per ricevere una notifica ogni volta che un log viene distribuito nel bucket. CloudTrail memorizza più eventi in un file di log. Le notifiche SNS vengono inviate per ogni file di log, non per ogni evento. Per ulteriori informazioni, consulta Configurazione delle notifiche Amazon SNS per CloudTrail.

      Se abiliti le notifiche SNS, per Create a new SNS topic (Crea un nuovo argomento SNS) scegli New (Nuovo) per creare un argomento oppure scegli Existing (Esistente) per utilizzare un argomento esistente. Se si crea un percorso multiregionale, le notifiche SNS per le consegne di file di registro da tutte le regioni abilitate vengono inviate al singolo argomento SNS creato.

      Se scegli New (Nuovo), CloudTrail specifica un nome per il nuovo argomento, in alternativa puoi digitare un nome. Se scegli Existing (Esistente), seleziona un argomento SNS dall'elenco a discesa. È anche possibile immettere l'ARN di un argomento da un'altra regione o da un account con le autorizzazioni appropriate. Per ulteriori informazioni, consulta Policy tematica di Amazon SNS per CloudTrail.

      Se si crea un argomento, è necessario sottoscrivere l'argomento per ricevere le notifiche di distribuzione dei file di log. Puoi abilitare la sottoscrizione nella console Amazon SNS. Data

la frequenza delle notifiche, ti consigliamo di configurare la sottoscrizione in modo da usare una coda Amazon SQS per gestire le notifiche a livello di programmazione. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

8. Facoltativamente, configura CloudTrail l'invio dei file di registro ai CloudWatch registri selezionando Abilitato nei registri. CloudWatch Per ulteriori informazioni, consulta Invio di eventi ai registri CloudWatch .

   a. Se abiliti l'integrazione con CloudWatch i log, scegli New (Nuovo) per creare un nuovo gruppo di log o Existing (Esistente) per utilizzarne uno esistente. Se scegli New (Nuovo), CloudTrail specifica un nome per il nuovo gruppo di log, in alternativa puoi digitare un nome.

   b. Se scegli Existing (Esistente), seleziona un gruppo di log dall'elenco a discesa.

   c. Scegli New (Nuovo) per creare un nuovo ruolo IAM per le autorizzazioni per inviare i log a CloudWatch Logs. Scegli Existing (Esistente) per selezionare un ruolo IAM esistente dall'elenco a discesa. L'istruzione della policy per il ruolo nuovo o esistente viene visualizzata quando espandi Policy document (Documento della policy). Per ulteriori informazioni su questo ruolo, consulta Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio.

   > **Note**
   >
   > - Durante la configurazione di un percorso, puoi scegliere un bucket S3 e un argomento SNS appartenenti a un altro account. Tuttavia, se desideri CloudTrail distribuire gli eventi a un gruppo di CloudWatch log di log, devi selezionare un gruppo di log esistente nell'account corrente.
   > - Solo l'account di gestione può configurare un gruppo di CloudWatch log di log per un percorso dell'organizzazione utilizzando la console. L'amministratore delegato può configurare un gruppo di log CloudWatch Logs utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API.

9. Per Tags (Tag), puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso al percorso. I tag consentono di identificare sia i CloudTrail percorsi che i bucket Amazon S3 contenenti CloudTrail file di log. Puoi quindi utilizzare i gruppi di risorse per le CloudTrail risorse. Per ulteriori informazioni, consultare AWS Resource Groups e Tag.

10. Nella pagina Choose log events (Seleziona eventi di log) seleziona i tipi di evento che vuoi registrare. Per Management events (Eventi di gestione), procedere nel seguente modo.

a. Per API activity (Attività API), scegli se vuoi che il percorso registri eventi Read (Lettura), Write (Scrittura) o entrambi. Per ulteriori informazioni, consulta Eventi di gestione.

b. Scegli Exclude AWS KMS events AWS Key Management Service (Escludi eventi AWS KMS KMS) per escludere gli eventi () dal percorso. L'impostazione predefinita è includere tutti gli AWS KMS eventi.

   L'opzione per registrare o escludere AWS KMS gli eventi è disponibile solo se registri gli eventi di gestione sul percorso. Se scegli di non registrare gli eventi di gestione, AWS KMS gli eventi non vengono registrati e non puoi modificare le impostazioni di registrazione AWS KMS degli eventi.

   AWS KMS azioni come `EncryptDecrypt`, e `GenerateDataKey` in genere generano un volume elevato (oltre il 99%) di eventi. Queste operazioni vengono ora registrate come eventi Read (Lettura). AWS KMS Le operazioni a basso volume pertinenti **`DisableDelete`**, come e **`ScheduleKey`** (che in genere rappresentano meno dello 0,5% del volume degli AWS KMS eventi), vengono registrate come eventi Write (Scrittura).

   Per escludere eventi a volume elevato come `EncryptDecrypt`, and`GenerateDataKey`, ma registrare comunque eventi rilevanti come `Delete` e `DisableScheduleKey`, scegli di registrare gli eventi di gestione Scrittura e deseleziona la casella di controllo Escludi AWS KMS eventi.

c. Scegli Exclude Amazon RDS Data API events (Escludi eventi dell'API dati di Amazon RDS) per escludere dal percorso gli eventi dell'API dati di Amazon Relational Database Service. L'impostazione predefinita è includere tutti gli eventi dell'API dati di Amazon RDS. Per ulteriori informazioni sugli eventi dell'API dati di Amazon RDS, consulta Registrazione delle chiamate dell'API dati con AWS CloudTrail nella Guida per l'utente di Amazon RDS per Aurora.

11. Per registrare gli eventi di dati, scegli Data events (Eventi di dati). Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

12.

> **Important**
>
> I passaggi 12-16 riguardano la configurazione degli eventi di dati tramite selettori di eventi avanzati, che sono l'impostazione predefinita. I selettori di eventi avanzati consentono di configurare più tipi di risorse e offrono un controllo dettagliato sugli eventi di dati acquisiti dal percorso. Se hai scelto di utilizzare i selettori di eventi di

base, completa i passaggi indicatiConfigurazione delle impostazioni degli eventi di dati utilizzando i selettori di eventi di base, quindi torna al passaggio 17 di questa procedura.

Per Tipo di risorsa (Tipo di risorsa), scegli il tipo di risorsa su cui desideri registrare gli eventi di dati. Per ulteriori informazioni sui tipi di risorse disponibili, consultaEventi di dati.

13. Scegli un modello di selettore di registro. Puoi scegliere un modello predefinito o scegliere Personalizzato per definire le condizioni di raccolta degli eventi.

    Puoi scegliere tra le seguenti opzioni predefinite:

    - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
    - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
    - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
    - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
    - Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

    > **Note**
    >
    > La selezione di un modello predefinito per i bucket S3 consente di registrare gli eventi di dati per tutti i bucket attualmente nell' AWS account e in qualsiasi bucket creato dopo aver ultimato la creazione del percorso. Verrà inoltre abilitata la registrazione dell'attività degli eventi di dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se l'attività viene eseguita in un bucket appartenente a un altro AWS account.
    > Se il percorso è valido solo per una regione, la selezione di un modello predefinito che registra tutti i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non verranno registrati gli eventi di dati per i bucket Amazon S3 nelle altre regioni dell'account. AWS

Se stai creando un percorso multiregione, la selezione di un modello predefinito per le funzioni Lambda consente la registrazione degli eventi di dati per tutte le funzioni attualmente nell'account AWS e qualsiasi funzione Lambda che puoi creare in qualsiasi regione dopo aver creato il percorso. Se stai creando un percorso per una singola regione (operazione eseguita tramite la AWS CLI), questa selezione consente la registrazione degli eventi di dati per tutte le funzioni attualmente in tale regione nell' AWS account e di qualsiasi funzione Lambda che puoi creare in tale regione dopo aver creato il percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
La registrazione degli eventi di dati per tutte le funzioni abilita anche la registrazione dell'attività degli eventi di dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se l'attività viene eseguita su una funzione appartenente a un altro AWS account.

14. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
15. Se hai selezionato Personalizzato, in Advanced event selectors crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

a. Scegli tra i seguenti campi.

- **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.
- **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`

- **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.
- eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete
- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.ARN`, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.ARN` campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

b. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere eventi di dati per due bucket S3 dagli eventi di dati registrati nel datastore di eventi, puoi impostare il campo su resources.ARN, impostare l'operatore per (Non inizia con) e quindi incollare in un ARN di un bucket S3 per il quale non desideri registrare eventi.

   Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

   CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

c. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

16. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi di dati, scegli Add data event type (Aggiungi tipo di evento di dati). Ripeti i passaggi da 12 a questo passaggio per configurare i selettori di eventi avanzati per il tipo di risorsa.

17. Per registrare gli eventi di attività di rete, scegli Eventi di attività di rete. Gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Per la registrazione degli eventi di attività di rete sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

    Per registrare gli eventi di attività di rete, procedi nel seguente modo:

    a. Da Origine eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.

    b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.

    c. (Facoltativo) Inserisci un nome per identificare il selettore. Il nome del selettore è riportato come Name nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

    d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

        i. Per escludere o includere gli eventi di attività di rete, puoi scegliere tra le seguenti opzioni nella console.

- **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi utilizzarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
- **`errorCode`**— È possibile utilizzarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.
- **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

18. Scegli Insights events (Eventi Insights) se desideri che il percorso registri gli eventi CloudTrail Insights.

    In Event type (Tipo di evento), seleziona Insights events (Eventi Insights). Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.

    CloudTrail Insights analizza la gestione degli eventi per individuare eventuali attività insolite e registra gli eventi quando vengono rilevate anomalie. Per impostazione predefinita, i trail non registrano gli eventi Insights. Per ulteriori informazioni sugli eventi Insights, consulta Lavorare con CloudTrail Insights. Per la registrazione degli eventi Insights vengono applicati costi aggiuntivi. Per i CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

    Gli eventi Insights vengono distribuiti in una cartella diversa denominata `/CloudTrail-Insight` con lo stesso bucket S3 specificato nell'area Storage location (Posizione di storage) della pagina dei dettagli del percorso. CloudTrailcrea il nuovo prefisso per l'utente. Ad esempio, se il bucket S3 di destinazione corrente è denominato `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`, il nome del bucket S3 con un nuovo prefisso viene denominato `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`.

19. Al termine della scelta dei tipi di evento da registrare, scegli Next (Successivo).

20. Nella pagina Review and create (Verifica e crea), esamina le opzioni selezionate. Scegli Edit (Modifica) in una sezione per modificare le impostazioni del percorso mostrate al suo interno. Quando sei pronto per creare il percorso, scegli Create trail (Crea percorso).
21. Il nuovo trail viene visualizzato nella pagina Trails (Trail). In circa 5 minuti, CloudTrail pubblica i file di log contenenti le chiamate AWS API effettuate nel tuo account. È possibile visualizzare i file di log nel bucket S3 specificato.

    Se hai abilitato gli eventi Insights per un percorso, CloudTrail potrebbero essere necessarie fino a 36 ore per iniziare a fornire questi eventi, a condizione che venga rilevata un'attività insolita durante quel periodo.

    > **Note**
    >
    > CloudTrail In genere, distribuisce i log con una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail.
    > Se configuri erroneamente il percorso (ad esempio, il bucket S3 è irraggiungibile), CloudTrail tenterà di inviare di nuovo i file di log al bucket S3 per 30 giorni e per questi attempted-to-deliver eventi saranno applicati i costi standard. CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Configurazione delle impostazioni degli eventi di dati utilizzando i selettori di eventi di base

Puoi utilizzare selettori di eventi avanzati per configurare tutti i tipi di eventi relativi ai dati e gli eventi di attività di rete. I selettori di eventi avanzati consentono di creare selettori dettagliati per registrare solo gli eventi di interesse.

Se utilizzi i selettori di eventi di base per registrare gli eventi di dati, sei limitato a registrare gli eventi di dati per i bucket Amazon S3 AWS Lambda , le funzioni e le tabelle Amazon DynamoDB. Non puoi filtrare sul campo utilizzando selettori di eventi di base. `eventName` Inoltre, non puoi registrare gli eventi di attività di rete.

Utilizza la seguente procedura per configurare le impostazioni degli eventi di dati utilizzando i selettori di eventi di base.

Configurazione delle impostazioni degli eventi di dati utilizzando i selettori di eventi di base

1. In Eventi, scegli Eventi di dati per registrare gli eventi di dati. Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.
2. Per i bucket Amazon S3:
   a. Per Data event source (Origine evento di dati), scegli S3.
   b. Puoi scegliere di registrare All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) oppure puoi specificare bucket o funzioni specifici. Per impostazione predefinita, gli eventi di dati vengono registrati per tutti i bucket S3 attuali e futuri.

      > **Note**
      >
      > La selezione dell'opzione predefinita All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) consente di registrare gli eventi di dati per tutti i bucket attualmente nell' AWS account e in qualsiasi bucket creato dopo aver ultimato la creazione del percorso. Verrà inoltre abilitata la registrazione dell'attività degli eventi di dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se l'attività viene eseguita in un bucket appartenente a un altro AWS account.
      > Se stai creando un percorso per una singola regione (operazione eseguita tramite la AWS CLI), la selezione di All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non verranno registrati gli eventi di dati per i bucket Amazon S3 nelle altre regioni dell'account. AWS

   c. Se lasci l'impostazione predefinita All current and future S3 buckets (Tutti i bucket S3 attuali e futuri), scegli di registrare gli eventi Read (Lettura), Write (Scrittura) o entrambi.
   d. Per selezionare singoli bucket, deseleziona le caselle di controllo Read (Lettura) e Write (Scrittura) per All current and future S3 buckets (Tutti i bucket S3 attuali e futuri). In Individual bucket selection (Selezione di singoli bucket), cerca un bucket in cui registrare gli eventi di dati. Puoi trovare bucket specifici digitando un prefisso del bucket per il bucket desiderato. Puoi selezionare più bucket in questa finestra. Scegli Add bucket (Aggiungi bucket) per registrare eventi di dati per più bucket. Scegli di registrare gli eventi Read (Lettura), ad esempio `GetObject`, gli eventi Write (Scrittura), ad esempio `PutObject`, oppure entrambi.

Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascun bucket. Ad esempio, se specifichi la registrazione degli eventi di lettura (Read) per tutti i buckets S3 e quindi scegli di aggiungere un bucket specifico per la registrazione degli eventi di dati, l'opzione Read (Lettura) è già selezionata per il bucket aggiunto. Non è possibile eliminare la selezione. Puoi solo configurare l'opzione Write (Scrittura).

Per rimuovere un bucket dalla registrazione, scegli X.

3. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi di dati, scegli Add data event type (Aggiungi tipo di evento di dati).
4. Per le funzioni Lambda:

   a. Per Data event source (Origine evento di dati), scegli Lambda.

   b. In Lambda function (Funzione Lambda), scegli All regions (Tutte le regioni) per registrare tutte le funzioni Lambda o Input function as ARN (Inserire la funzione come ARN) per registrare eventi di dati su una funzione specifica.

   Per registrare eventi di dati per tutte le funzioni Lambda nell' AWS account, seleziona Log all current and future functions (Registra tutte le funzioni presenti e future). Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascuna funzione. Tutte le funzioni vengono registrate, anche se tutte le funzioni non vengono visualizzate.

   > **Note**
   >
   > Se stai creando un percorso multiregione, questa selezione consente la registrazione degli eventi di dati per tutte le funzioni attualmente nell' AWS account e qualsiasi funzione Lambda che puoi creare in qualsiasi regione dopo aver creato il percorso. Se stai creando un percorso per una singola regione (operazione eseguita tramite la AWS CLI), questa selezione consente la registrazione degli eventi di dati per tutte le funzioni attualmente in tale regione nell' AWS account e di qualsiasi funzione Lambda che puoi creare in tale regione dopo aver creato il percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
   > La registrazione degli eventi di dati per tutte le funzioni abilita anche la registrazione dell'attività degli eventi di dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se l'attività viene eseguita su una funzione appartenente a un altro AWS account.

c. Se scegli Input function as ARN (Inserire la funzione come ARN), immetti l'ARN di una funzione Lambda.

> **Note**
>
> Se sono presenti più di 15.000 funzioni Lambda nell'account, non puoi visualizzare o selezionare tutte le funzioni nella console durante CloudTrail la creazione di un percorso. Puoi comunque selezionare l'opzione che consente di registrare tutte le funzioni, anche se non sono visualizzate. Se desideri registrare gli eventi di dati per funzioni specifiche, puoi aggiungere manualmente una funzione di cui conosci l'ARN. Puoi anche ultimare la creazione del percorso nella console e quindi utilizzare il AWS CLI put-event-selectors comando and per configurare la registrazione degli eventi di dati per funzioni Lambda specifiche. Per ulteriori informazioni, consulta Gestire i percorsi con AWS CLI.

5. Per le tabelle Dynamo DB:

   a. Per Data event source (Origine evento di dati), scegli Dynamo DB.

   b. In DynamoDB table selection (Selezione tabella Dynamo DB), scegli Browse (Sfoglia) per selezionare una tabella o incolla l'ARN di una tabella Dynamo DB a cui hai accesso. L'ARN di una tabella Dynamo DB ha il seguente formato:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   Per aggiungere un'altra tabella, scegli Add row (Aggiungi riga) e cerca una tabella o incolla l'ARN di una tabella a cui hai accesso.

6. Per configurare gli eventi Insights e altre impostazioni per il percorso, torna alla procedura precedente in questo argomento, ???.

Passaggi successivi

Dopo aver creato il trail, è possibile tornare al trail per apportarvi modifiche:

- Se non lo hai già fatto, puoi configurare CloudTrail l'invio dei file di log a CloudWatch Logs. Per ulteriori informazioni, consulta Invio di eventi ai registri CloudWatch .

- Crea una tabella e utilizzala per eseguire una query in Amazon Athena per analizzare le attività del servizio AWS . Per ulteriori informazioni, consulta Creare una tabella per CloudTrail i log nella CloudTrail console nella Guida per l'utente di Amazon Athena.
- Aggiungere tag (coppie chiave-valore) personalizzati al trail.
- Per creare un altro percorso, apri la pagina Percorsi e scegli Aggiungi nuovo percorso.

Aggiornamento di un percorso con la CloudTrail console

Questa sezione descrive come modificare le impostazioni del percorso.

Per convertire un percorso basato su una singola Regione o aggiornare un percorso multi-regione per registrare eventi in una sola regione, devi utilizzare la. AWS CLI Per ulteriori informazioni su come convertire un percorso basato su una singola Regione in un percorso multi-regione, consulta. Conversione di un percorso a regione singola in un percorso multiregionale Per ulteriori informazioni su come aggiornare un percorso multi-regione per registrare eventi in una sola regione, consultaConversione di un percorso multi-regione in un percorso basato su una Regione singola.

Se hai abilitato gli eventi di CloudTrail gestione in Amazon Security Lake, devi mantenere almeno un percorso dell'organizzazione multi-regione che registri `read` sia gli eventi di `write` gestione. Non puoi aggiornare un percorso qualificante in modo che non soddisfi i requisiti di Security Lake. Ad esempio, modificando il percorso in Regione singola o disattivando la registrazione degli eventi di gestione `read` o `write`.

> **Note**
>
> CloudTrail aggiorna gli itinerari organizzativi negli account dei membri anche se la convalida di una risorsa fallisce. Alcuni esempi di errori di convalida includono:
>
> - una policy del bucket Amazon S3 non corretta
> - una policy degli argomenti Amazon SNS non corretta
> - impossibilità di effettuare consegne a un gruppo di CloudWatch log di Logs
> - autorizzazione insufficiente per crittografare utilizzando una chiave KMS
>
> Un account membro con CloudTrail autorizzazioni può visualizzare eventuali errori di convalida di un percorso organizzativo visualizzando la pagina dei dettagli del percorso sulla CloudTrail console o eseguendo il comando. AWS CLI get-trail-status

Per aggiornare un percorso con AWS Management Console

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione, scegli Trails (Percorsi) e quindi scegli il nome del percorso.
3. In General details (Dettagli generali), scegli Edit (Modifica) per modificare le impostazioni seguenti. Non puoi modificare il nome di un percorso.

   - Apply trail to my organization (Applica percorso all'organizzazione): modifica questo percorso in un percorso di AWS Organizations organizzazione.

     > **Note**
     >
     > Solo l'account di gestione dell'organizzazione può convertire un percorso dell'organizzazione in un percorso non dell'organizzazione o viceversa.

   - Trail log location (Posizione del log di percorso): cambia il nome del bucket S3 o del prefisso in cui archivi i registri per questo percorso.
   - Log file SSE-KMS encryption (Crittografia SSE-KMS dei file di log): scegli di abilitare o disabilitare la crittografia dei file di log con SSE-KMS anziché con SSE-S3.
   - Log file validation(Abilita la convalida dei file di log): scegli di abilitare o disabilitare la convalida dell'integrità dei file di log.
   - SNS notification delivery (Consegna delle notifiche SNS): scegli di abilitare o disabilitare le notifiche di Amazon Simple Notification Service (Amazon SNS) che segnalano che i file di log sono stati consegnati al bucket specificato per il percorso.

   a. Per modificare il percorso in un percorso di AWS Organizations organizzazione, puoi scegliere di abilitare il percorso per tutti gli account presenti nell'organizzazione. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione.

   b. Per modificare il bucket specificato in Storage location (Posizione di storage), scegli Create new S3 bucket (Crea nuovo bucket S3) per creare un bucket. Quando crei un bucket, CloudTrail crea e applica le policy del bucket obbligatorie. Se scegli di creare un nuovo bucket S3, la tua policy IAM deve includere l'autorizzazione per l'`s3:PutEncryptionConfiguration`azione perché per impostazione predefinita la crittografia lato server è abilitata per il bucket.

> **Note**
>
> Se scegli Use existing S3 bucket (Utilizza bucket S3 esistente), specifica un bucket in Trail log bucket name (Nome del bucket del log del percorso), oppure scegli Browse (Sfoglia) per scegliere un bucket. La policy del bucket deve concedere CloudTrail il permesso di scrittura nel bucket stesso. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket Amazon S3 per CloudTrail.

Per semplificare la ricerca dei registri, creare una nuova cartella (nota anche come prefisso) in un bucket esistente per archiviare i registri. CloudTrail Inserire il prefisso in Prefix (Prefisso).

c. Per Log file SSE-KMS encryption (Crittografia SSE-KMS dei file di log), scegli Enabled (Abilitata) per crittografare i file di log e i file digest tramite SSE-KMS anziché con SSE-S3. L'impostazione predefinita è Enabled (Abilitata). Se non abiliti la crittografia SSE-KMS, i file di log e i file digest vengono crittografati utilizzando la crittografia SSE-S3. Per ulteriori informazioni sulla crittografia SSE-KMS, consulta Utilizzo della crittografia lato server con (SSE-KMS). AWS Key Management Service Per ulteriori informazioni sulla crittografia SSE-S3, consulta Utilizzo della crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3).

   Se abiliti la crittografia SSE-KMS, scegli Nuova o Esistente. AWS KMS key In AWS KMS Alias (Alias KMS), specifica un alias, nel formato. `alias/` *`MyAliasName`* Per ulteriori informazioni, consultaAggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. CloudTrail supporta anche chiavi AWS KMS multi-regione. Per ulteriori informazioni sulle chiavi multi-regione, consulta Utilizzo delle chiavi multi-regione nella Guida per gli sviluppatori di AWS Key Management Service .

> **Note**
>
> È anche possibile digitare l'ARN di una chiave da un altro account. Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. La policy della chiave deve CloudTrail permettere di utilizzare la chiave per crittografare i file di log e i file digest e permettere agli utenti specificati di leggere i file di log o i file digest in formato non crittografato. Per informazioni sulla

modifica manuale della policy della chiave, consulta Configura le politiche AWS KMS chiave per CloudTrail.

d. In Enable log file validation (Abilita la convalida dei file di log), scegli Enabled (Abilitata) per attivare la distribuzione dei file digest di log nel bucket S3. Puoi utilizzare i file digest per verificare che i file di log non siano stati CloudTrail modificati dopo essere stati distribuiti. Per ulteriori informazioni, consulta Convalida dell'integrità dei file di CloudTrail registro.

e. Per SNS notification delivery (Consegna delle notifiche SNS), scegli Enabled (Abilitata) per ricevere una notifica ogni volta che un log viene distribuito nel bucket. CloudTrail memorizza più eventi in un file di log. Le notifiche SNS vengono inviate per ogni file di log, non per ogni evento. Per ulteriori informazioni, consulta Configurazione delle notifiche Amazon SNS per CloudTrail.

   Se abiliti le notifiche SNS, per Create a new SNS topic (Crea un nuovo argomento SNS) scegli New (Nuovo) per creare un argomento oppure scegli Existing (Esistente) per utilizzare un argomento esistente. Se si crea un percorso multiregionale, le notifiche SNS per le consegne di file di registro da tutte le regioni abilitate vengono inviate al singolo argomento SNS creato.

   Se scegli New (Nuovo), CloudTrail specifica un nome per il nuovo argomento, in alternativa puoi digitare un nome. Se scegli Existing (Esistente), seleziona un argomento SNS dall'elenco a discesa. È anche possibile immettere l'ARN di un argomento da un'altra regione o da un account con le autorizzazioni appropriate. Per ulteriori informazioni, consulta Policy tematica di Amazon SNS per CloudTrail.

   Se si crea un argomento, è necessario sottoscrivere l'argomento per ricevere le notifiche di distribuzione dei file di log. Puoi abilitare la sottoscrizione nella console Amazon SNS. Data la frequenza delle notifiche, ti consigliamo di configurare la sottoscrizione in modo da usare una coda Amazon SQS per gestire le notifiche a livello di programmazione. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

4. In CloudWatch Registri, scegli Modifica per modificare le impostazioni per l'invio dei file di CloudTrail registro ai CloudWatch registri. Scegli Abilitato nei CloudWatch registri per abilitare l'invio di file di registro. Per ulteriori informazioni, consulta Invio di eventi ai registri CloudWatch .

a. Se abiliti l'integrazione con CloudWatch Logs (Nuovo) per creare un nuovo gruppo di log o Existing (Esistente) per utilizzarne uno esistente. Se scegli New (Nuovo), CloudTrail specifica un nome per il nuovo gruppo di log, in alternativa puoi digitare un nome.

b. Se scegli Existing (Esistente), seleziona un gruppo di log dall'elenco a discesa.

c. Scegli New (Nuovo) per creare un nuovo ruolo IAM per le autorizzazioni per inviare i log ai CloudWatch registri. Scegli Existing (Esistente) per selezionare un ruolo IAM esistente dall'elenco a discesa. L'istruzione della policy per il ruolo nuovo o esistente viene visualizzata quando espandi Policy document (Documento della policy). Per ulteriori informazioni su questo ruolo, consulta Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio.

> **Note**
>
> - Durante la configurazione di un percorso, puoi scegliere un bucket S3 e un argomento SNS appartenenti a un altro account. Tuttavia, se desideri inviare eventi CloudTrail a un gruppo di log di CloudWatch Logs, devi selezionare un gruppo di log esistente nell'account corrente.
> - Solo l'account di gestione può configurare un gruppo di log di CloudWatch Logs per un percorso dell'organizzazione utilizzando la console. L'amministratore delegato può configurare un gruppo di log CloudWatch Logs utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API.

5. In Tags (Tag), scegli Edit (Modifica) per modificare, aggiungere o eliminare tag nel percorso. Puoi aggiungere fino a 50 coppie di chiavi di tag per identificare, ordinare e controllare l'accesso al percorso. I tag consentono di identificare sia i CloudTrail percorsi che i bucket Amazon S3 contenenti CloudTrail file di log. Puoi quindi utilizzare i gruppi di risorse per le CloudTrail risorse. Per ulteriori informazioni, consultare AWS Resource Groups e Tag.

6. In Management events (Eventi di gestione), scegli Edit (Modifica) per modificare le impostazioni di registrazione degli eventi di gestione.

   a. Per API activity (Attività API), scegli se vuoi che il percorso registri eventi Read (Lettura), Write (Scrittura) o entrambi. Per ulteriori informazioni, consulta Eventi di gestione.

   b. Scegli Exclude AWS KMS events AWS Key Management Service (Escludi eventi KMS AWS KMS) per escludere gli eventi () () dal percorso. L'impostazione predefinita è includere tutti gli eventi AWS KMS .

L'opzione per registrare o escludere AWS KMS gli eventi è disponibile solo se registri gli eventi di gestione sul percorso. Se scegli di non registrare gli eventi di gestione, AWS KMS gli eventi non vengono registrati e non puoi modificare le impostazioni di registrazione AWS KMS degli eventi.

AWS KMS azioni come `EncryptDecrypt`, e `GenerateDataKey` in genere generano un volume elevato (oltre il 99%) di eventi. Queste operazioni vengono ora registrate come eventi Read (Lettura). AWS KMS Le operazioni a basso volume pertinenti **`DisableDelete`**, come e **`ScheduleKey`** (che in genere rappresentano meno dello 0,5% del volume degli AWS KMS eventi), vengono registrate come eventi Write (Scrittura).

Per escludere eventi a volume elevato come `Encrypt`, `Decrypt` e `GenerateDataKey`, ma registrare comunque eventi rilevanti come `Disable`, `Delete` e `ScheduleKey`, scegli di registrare gli eventi di gestione Write (Scrittura) e deseleziona la casella di controllo Exclude AWS KMS events (Escludi eventi KMS).

c. Scegli Exclude Amazon RDS Data API events (Escludi eventi dell'API dati di Amazon RDS) per escludere dal percorso gli eventi dell'API dati di Amazon Relational Database Service. L'impostazione predefinita è includere tutti gli eventi dell'API dati di Amazon RDS. Per ulteriori informazioni sugli eventi dell'API dati di Amazon RDS, consulta Registrazione delle chiamate dell'API dati con AWS CloudTrail nella Guida per l'utente di Amazon RDS per Aurora.

7.

> **Important**
>
> I passaggi 7-11 riguardano la configurazione degli eventi di dati tramite selettori di eventi avanzati, che sono l'impostazione predefinita. I selettori di eventi avanzati consentono di configurare più tipi di eventi di dati e offrono un controllo dettagliato sugli eventi di dati acquisiti dal percorso. Se intendi registrare gli eventi di attività di rete, devi utilizzare i selettori di eventi avanzati. Se utilizzi selettori di eventi di base, consulta Aggiornamento delle impostazioni degli eventi di dati con selettori di eventi di base, quindi torna al passaggio 12 di questa procedura.

In Data events (Eventi di dati), scegli Edit (Modifica) per modificare le impostazioni di registrazione degli eventi di dati. Per impostazione predefinita, i trail non registrano gli eventi di dati Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per i prezzi CloudTrail, consulta Prezzi di AWS CloudTrail.

Per Tipo di risorsa, scegli il tipo di risorsa su cui desideri registrare gli eventi di dati. Per ulteriori informazioni sui tipi di risorse disponibili, consultaEventi di dati.

8. Scegli un modello di selettore di registro. Puoi scegliere un modello predefinito o scegliere Personalizzato per definire le condizioni di raccolta degli eventi.

   Puoi scegliere tra le seguenti opzioni predefinite:

   - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
   - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*` eventi.
   - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
   - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
   - Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

   > **Note**
   >
   > La selezione di un modello predefinito per i bucket S3 consente di registrare gli eventi di dati per tutti i bucket attualmente nell' AWS account e in qualsiasi bucket creato dopo aver ultimato la creazione del percorso. Verrà inoltre abilitata la registrazione dell'attività degli eventi di dati eseguita da qualsiasi utente o ruolo nel tuo AWS account, anche se l'attività viene eseguita in un bucket appartenente a un altro AWS account.
   > Se il percorso è valido solo per una regione, la selezione di un modello predefinito che registra tutti i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non verranno registrati gli eventi di dati per i bucket Amazon S3 nelle altre regioni dell'account AWS .
   > Se stai creando un percorso multiregione, la selezione di un modello predefinito per le funzioni Lambda consente la registrazione degli eventi di dati per tutte le funzioni attualmente nell'account AWS e qualsiasi funzione Lambda che puoi creare in qualsiasi

regione dopo aver creato il percorso. Se stai creando un percorso per una singola Regione (operazione eseguita tramite la AWS CLI), questa selezione consente la registrazione di tutte le funzioni attualmente in tale Regione nell' AWS account e di qualsiasi funzione Lambda che puoi creare in tale Regione dopo aver creato il percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
La registrazione degli eventi di dati per tutte le funzioni abilita anche la registrazione dell'attività degli eventi di dati eseguita da qualsiasi utente o ruolo nel tuo AWS account, anche se l'attività viene eseguita su una funzione appartenente a un altro AWS account.

9. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
10. Se hai selezionato Personalizzato, in Selettori di eventi avanzati crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

a. Scegli tra i seguenti campi.

- **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.
- **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`
- **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.

- eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete
- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.ARN`, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.ARN` campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

b. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere eventi di dati per due bucket S3 dagli eventi di dati registrati nel datastore di eventi, puoi impostare il campo su resources.ARN, impostare l'operatore per non inizia con e quindi incollare in un ARN di un bucket S3 per il quale non desideri registrare eventi.

   Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

   CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di

valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

c. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

11. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi di dati, scegli Add data event type (Aggiungi tipo di evento di dati). Ripeti i passaggi da 3 a questo passaggio per configurare i selettori di eventi avanzati per il tipo di risorsa.

12. In Eventi di attività di rete, scegli Modifica per modificare le impostazioni di registrazione degli eventi di attività di rete. Per impostazione predefinita, i percorsi non registrano gli eventi di attività di rete. Per la registrazione degli eventi di attività di rete vengono applicati costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

    Per registrare gli eventi di attività di rete, procedi come segue:

    a. Da Origine eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.

    b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.

    c. (Facoltativo) Inserisci un nome per identificare il selettore. Il nome del selettore è riportato come Name nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

    d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

        i. Per escludere o includere gli eventi di attività di rete, puoi scegliere tra le seguenti opzioni nella console.

            - **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi utilizzarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
            - **`errorCode`**— Puoi usarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.
            - **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

13. In Insights events (Eventi Insights), scegli Edit (Modifica) se desideri che il percorso registri gli eventi CloudTrail Insights.

    In Event type (Tipo di evento), seleziona Insights events (Eventi Insights).

    In Insights events (Eventi Insights), scegli API calls rate (Tasso di chiamata API), API error rate (Tasso di errore API), o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.

    CloudTrail Insights analizza la gestione degli eventi per individuare eventuali attività insolite e registra gli eventi quando vengono rilevate anomalie. Per impostazione predefinita, i trail non registrano gli eventi Insights. Per ulteriori informazioni sugli eventi Insights, consulta Lavorare con CloudTrail Insights. Per la registrazione degli eventi Insights vengono applicati costi aggiuntivi. Per i CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

    Gli eventi Insights vengono distribuiti in una cartella diversa denominata `/CloudTrail-Insight` con lo stesso bucket S3 specificato nell'area Storage location (Posizione di storage) della pagina dei dettagli del percorso. CloudTrailcrea il nuovo prefisso per l'utente. Ad esempio, se il bucket S3 di destinazione corrente è denominato `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`, il nome del bucket S3 con un nuovo prefisso viene denominato `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`.

14. Al termine della modifica delle impostazioni sul percorso, scegli Update trail (Aggiorna percorso).

Aggiornamento delle impostazioni degli eventi di dati con selettori di eventi di base

Puoi utilizzare selettori di eventi avanzati per configurare tutti i tipi di eventi relativi ai dati e gli eventi di attività di rete. I selettori di eventi avanzati consentono di creare selettori dettagliati per registrare solo gli eventi di interesse.

Se utilizzi i selettori di eventi di base per registrare gli eventi di dati, sei limitato a registrare gli eventi di dati per i bucket Amazon S3 AWS Lambda , le funzioni e le tabelle Amazon DynamoDB. Non puoi filtrare sul campo utilizzando selettori di eventi di base. `eventName` Inoltre, non puoi registrare gli eventi di attività di rete.

Utilizza la seguente procedura per configurare le impostazioni degli eventi di dati utilizzando i selettori di eventi di base.

1. In Data events (Eventi di dati), scegli Edit (Modifica) per modificare le impostazioni di registrazione degli eventi di dati. Con i selettori di eventi di base, puoi specificare la registrazione degli eventi di dati per i bucket Amazon S3 AWS Lambda , le funzioni, DBtables Dynamo o una combinazione di queste risorse. Altri tipi di risorse di eventi di dati sono supportati con selettori di eventi avanzati. Per impostazione predefinita, i trail non registrano gli eventi di dati Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta Eventi di dati. Per i prezzi CloudTrail, consulta Prezzi di AWS CloudTrail.

   Per i bucket Amazon S3:

   a. Per Data event source (Origine evento di dati), scegli S3.
   b. Puoi scegliere di registrare All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) oppure puoi specificare bucket o funzioni specifici. Per impostazione predefinita, gli eventi di dati vengono registrati per tutti i bucket S3 attuali e futuri.

   > **Note**
   >
   > La selezione dell'opzione predefinita All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) consente di registrare gli eventi di dati per tutti i bucket attualmente nell' AWS account e in qualsiasi bucket creato dopo aver ultimato la creazione del percorso. Verrà inoltre abilitata la registrazione dell'attività degli eventi di dati eseguita da qualsiasi utente o ruolo nel tuo AWS account, anche se l'attività viene eseguita in un bucket appartenente a un altro AWS account.

Se il percorso è valido solo per una regione, la selezione di All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non verranno registrati gli eventi di dati per i bucket Amazon S3 nelle altre regioni dell'account. AWS

c. Se lasci l'impostazione predefinita All current and future S3 buckets (Tutti i bucket S3 attuali e futuri), scegli di registrare gli eventi Read (Lettura), Write (Scrittura) o entrambi.

d. Per selezionare singoli bucket, deseleziona le caselle di controllo Read (Lettura) e Write (Scrittura) per All current and future S3 buckets (Tutti i bucket S3 attuali e futuri). In Individual bucket selection (Selezione di singoli bucket), cerca un bucket in cui registrare gli eventi di dati. Per trovare bucket specifici, digita un prefisso del bucket per il bucket desiderato. Puoi selezionare più bucket in questa finestra. Scegli Add bucket (Aggiungi bucket) per registrare eventi di dati per più bucket. Scegli di registrare gli eventi Read (Lettura), ad esempio `GetObject`, gli eventi Write (Scrittura), ad esempio `PutObject`, oppure entrambi.

   Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascun bucket. Ad esempio, se specifichi la registrazione degli eventi di lettura (Read) per tutti i buckets S3 e quindi scegli di aggiungere un bucket specifico per la registrazione degli eventi di dati, l'opzione Read (Lettura) è già selezionata per il bucket aggiunto. Non è possibile eliminare la selezione. Puoi solo configurare l'opzione Write (Scrittura).

   Per rimuovere un bucket dalla registrazione, scegli X.

2. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi di dati, scegli Add data event type (Aggiungi tipo di evento di dati).

3. Per le funzioni Lambda:

   a. Per Data event source (Origine evento di dati), scegli Lambda.

   b. In Lambda function (Funzione Lambda), scegli All regions (Tutte le regioni) per registrare tutte le funzioni Lambda o Input function as ARN (Inserire la funzione come ARN) per registrare eventi di dati su una funzione specifica.

   Per registrare gli eventi di dati per tutte le funzioni Lambda nell' AWS account, seleziona Log all current and future functions (Registra tutte le funzioni presenti e future). Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascuna funzione. Tutte le funzioni vengono registrate, anche se tutte le funzioni non vengono visualizzate.

> **Note**
>
> Se stai creando un percorso multi-regione, questa selezione consente la registrazione degli eventi di dati per tutte le funzioni attualmente nell' AWS account e qualsiasi funzione Lambda che puoi creare in qualsiasi regione dopo aver creato il percorso. Se stai creando un percorso per una singola Regione (operazione eseguita tramite la AWS CLI), questa selezione consente la registrazione di tutte le funzioni attualmente in tale Regione nell' AWS account e di qualsiasi funzione Lambda che puoi creare in tale Regione dopo aver creato il percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
> La registrazione degli eventi di dati per tutte le funzioni abilita anche la registrazione dell'attività degli eventi di dati eseguita da qualsiasi utente o ruolo nel tuo AWS account, anche se l'attività viene eseguita su una funzione appartenente a un altro AWS account.

c. Se scegli Input function as ARN (Inserire la funzione come ARN), immetti l'ARN di una funzione Lambda.

> **Note**
>
> Se nell'account sono presenti più di 15.000 funzioni Lambda, non puoi visualizzare o selezionare tutte le funzioni nella console durante CloudTrail la creazione di un percorso. Puoi comunque selezionare l'opzione che consente di registrare tutte le funzioni, anche se non sono visualizzate. Se desideri registrare gli eventi di dati per funzioni specifiche, puoi aggiungere manualmente una funzione di cui conosci l'ARN. Puoi anche ultimare la creazione del percorso nella console e quindi utilizzare la AWS CLI e il comando put-event-selectors per configurare la registrazione degli eventi di dati per funzioni Lambda specifiche. Per ulteriori informazioni, consulta Gestire i percorsi con AWS CLI.

4. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi di dati, scegli Add data event type (Aggiungi tipo di evento di dati).
5. Per le tabelle Dynamo DB:
   a. Per Data event source (Origine evento di dati), scegli Dynamo DB.

b. In DynamoDB table selection (Selezione tabella Dynamo DB), scegli Browse (Sfoglia) per selezionare una tabella o incolla l'ARN di una tabella Dynamo DB a cui hai accesso. L'ARN di una tabella Dynamo DB è nel seguente formato:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Per aggiungere un'altra tabella, scegli Add row (Aggiungi riga) e cerca una tabella o incolla l'ARN di una tabella a cui hai accesso.

6. Per configurare gli eventi Insights e altre impostazioni per il percorso, torna alla procedura precedente in questo argomento, Aggiornamento di un percorso con la CloudTrail console.

Eliminazione di un percorso con la console CloudTrail

È possibile eliminare i percorsi con la CloudTrail console. Se l'account di gestione di un'organizzazione o l'account dell'amministratore delegato elimina un trail dell'organizzazione, questo viene rimosso da tutti gli account dei membri dell'organizzazione.

Se hai abilitato gli eventi di CloudTrail gestione in Amazon Security Lake, devi mantenere almeno un percorso organizzativo multiregionale e registrare sia `read` gli eventi che gli eventi di `write` gestione. Non puoi eliminare un trail se è l'unico a tua disposizione che soddisfa questo requisito, a meno che non disattivi gli eventi di CloudTrail gestione in Security Lake.

Per eliminare un trail con la CloudTrail console

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Apri la pagina Trails della CloudTrail console.
3. Scegliere il nome del trail.
4. Nella parte superiore della pagina dei dettagli del percorso, scegli Delete (Elimina).
5. Quando viene richiesto di confermare l'operazione, scegli Delete (Elimina) per eliminare definitivamente il percorso. Il percorso viene rimosso dall'elenco dei percorsi. I file di log che sono già stati consegnati al bucket Amazon S3 non vengono eliminati e continuano a comportare costi S3.

> **Note**
>
> I contenuti distribuiti ai bucket Amazon S3 potrebbero contenere informazioni dei clienti. Per ulteriori informazioni sulla rimozione di dati sensibili, consulta Svuotare un bucket ed Eliminare un bucket nella Amazon S3 User Guide.

Disattivazione della registrazione per un percorso

Quando crei un trail, la registrazione viene attivata automaticamente. Puoi disattivare la registrazione di un percorso dalla pagina dei dettagli del percorso.

> **Note**
>
> Quando disattivi la registrazione, i log esistenti sono ancora archiviati nel bucket Amazon S3 del percorso e continuano a comportare costi S3. Per informazioni sui prezzi di S3, consulta i prezzi di Amazon S3.

Per disattivare la registrazione di un percorso con la console CloudTrail

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione, scegli Trails (Percorsi) e quindi scegli il nome del percorso.
3. Nella parte superiore della pagina dei dettagli del percorso, scegli Stop Logging (Interrompi la registrazione) per disattivare la registrazione per il percorso.
4. Quando ti viene richiesto di confermare, scegli Stop logging. CloudTrailinterrompe la registrazione dell'attività per quel percorso.
5. Per riprendere la registrazione per il percorso, scegli Start logging (Avvia la registrazione) nella pagina di configurazione del percorso.

Creazione, aggiornamento e gestione di percorsi con AWS CLI

Puoi usare il AWS CLI per creare, aggiornare e gestire i tuoi percorsi. Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella AWS regione configurata per il tuo profilo. Per eseguire

i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

> **Note**
>
> Sono necessari gli strumenti della riga di AWS comando per eseguire i comandi AWS Command Line Interface (AWS CLI) descritti in questo argomento. Accertatevi di avere AWS CLI installato una versione recente del file. Per ulteriori informazioni, consulta la Guida per l'utente AWS Command Line Interface. Per informazioni sui CloudTrail comandi nella AWS CLI riga di comando, digitate`aws cloudtrail help`.

I comandi comunemente utilizzati per creazione, la gestione e lo stato

Alcuni dei comandi più comunemente usati per creare e aggiornare i percorsi CloudTrail includono:

- create-trail per creare un trail.
- update-trail per modificare la configurazione di un trail esistente.
- add-tags per aggiungere uno o più tag (coppie chiave-valore) a un trail esistente.
- remove-tags per rimuovere uno o più tag da un trail.
- list-tags per ottenere un elenco di tag associati a un trail.
- put-event-selectors per aggiungere o modificare selettori per un evento per un trail.
- put-insight-selectors per aggiungere o modificare i selettori di eventi Insights per un trail esistente e abilitare o disabilitare gli eventi Insights.
- start-logging per avviare la registrazione degli eventi con il trail.
- stop-logging per interrompere la registrazione degli eventi con il trail.
- delete-trail per eliminare un trail. Questo comando non elimina il bucket Amazon S3 che contiene i file di log per il percorso, se presenti.
- describe-trailsper restituire informazioni sui sentieri in una AWS regione.
- get-trail per restituire informazioni sulle impostazioni per un trail.
- get-trail-status per restituire informazioni sullo stato corrente di un trail.
- get-event-selectors per raccogliere le informazioni sui selettori evento configurati per un trail.
- get-insight-selectors per raccogliere le informazioni sui selettori dell'evento Insights configurati per un trail.

I comandi supportati per la creazione e l'aggiornamento dei trail: create-trail e aggiornare-trail

I comandi `update-trail` e `create-trail` offrono un'ampia gamma di funzionalità per la creazione e la gestione di trail, tra cui:

- Creazione di un trail che riceve i log da tutte le regioni o aggiornamento di un trail mediante l'opzione `--is-multi-region-trail`. Nella maggior parte dei casi, è necessario creare percorsi che registrino gli eventi in tutte le AWS regioni.
- Creazione di un percorso che riceva i log di tutti AWS gli account di un'organizzazione con l'--is-organization-trailopzione.
- Conversione di un percorso multi-regione in un percorso basato su una regione singola mediante l'opzione `--no-is-multi-region-trail`.
- L'abilitazione o la disabilitazione della crittografia dei file di log con l'opzione`--kms-key-id`. L'opzione specifica una AWS KMS chiave già creata e alla quale è stata allegata una politica che consente di CloudTrail crittografare i log. Per ulteriori informazioni, consulta Abilitazione e disabilitazione della crittografia per file di CloudTrail registro, file digest e archivi di dati di eventi con AWS CLI.
- L'abilitazione o la disabilitazione della convalida dei file di log con le opzioni `--enable-log-file-validation` e `--no-enable-log-file-validation`. Per ulteriori informazioni, consulta Convalida dell'integrità dei file di CloudTrail registro.
- Specificare un gruppo e un ruolo di log CloudWatch Logs in modo da CloudTrail poter fornire eventi a un gruppo di log Logs. CloudWatch Per ulteriori informazioni, consulta Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs.

Comandi obsoleti: create-subscription e update-subscription

> **Important**
>
> I comandi `update-subscription` e `create-subscription` sono stati usati per creare e aggiornare trail, ma sono obsoleti. Non utilizzare questi comandi. Essi non offrono funzionalità complete per la creazione e la gestione di trail.
> Se hai configurato l'automazione che utilizza uno di questi comandi o entrambi, ti consigliamo di aggiornare il codice o gli script per l'utilizzo di comandi supportati, ad esempio create-trail.

Utilizzo del **`create-trail`** comando per creare una traccia

Puoi eseguire il comando `create-trail` per creare percorsi configurati appositamente per soddisfare le esigenze aziendali. Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella AWS regione configurata per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Creazione di un percorso multiregionale

Un percorso può essere applicato a tutto ciò Regioni AWS che è abilitato nella tua Account AWS o può essere applicato a una singola regione. Un percorso che si applica a tutto Regioni AWS ciò che è abilitato nella tua Account AWS viene definito percorso multiregionale. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate.

Per creare un percorso multiregionale, utilizza l'opzione. `--is-multi-region-trail` Per impostazione predefinita, il comando `create-trail` crea un trail che registra solo gli eventi all'interno della regione AWS in cui il trail è stato creato. Per assicurarti di registrare gli eventi di servizio globali e acquisire tutte le attività relative agli eventi di gestione nel tuo AWS account, devi creare percorsi che registrino gli eventi in tutte le AWS regioni.

> **Note**
>
> Quando crei un trail, se specifichi un bucket Amazon S3 che non è stato creato con CloudTrail, devi allegare la policy appropriata. Per informazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.

L'esempio seguente crea un percorso multiregionale con il nome *`my-trail`* e un tag con una chiave denominata *`Group`* con un valore di *`Marketing`* che invia i log di tutte le regioni abilitate del tuo account a un bucket esistente denominato. *`amzn-s3-demo-bucket`*

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
multi-region-trail --tags-list [key=Group,value=Marketing]
```

Per confermare che il percorso è un percorso multiregionale, verifica che l'`IsMultiRegionTrail`elemento nell'output sia visualizzato. `true`

```
{
    "IncludeGlobalServiceEvents": true,
```

```
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

> **Note**
>
> Usa il comando `start-logging` per avviare la registrazione per il trail.

Avvio della registrazione per il trail

Dopo il completamento dell'esecuzione del comando `create-trail`, eseguir il comando `start-logging` per avviare la registrazione per il trail.

> **Note**
>
> Quando crei un percorso con la CloudTrail console, la registrazione viene attivata automaticamente.

L'esempio seguente avvia la registrazione per un trail.

```
aws cloudtrail start-logging --name my-trail
```

Questo comando non restituisce un output, ma puoi utilizzare il comando `get-trail-status` per verificare se la registrazione è stata avviata.

```
aws cloudtrail get-trail-status --name my-trail
```

A conferma che il trail sta eseguendo la registrazione, l'elemento `IsLogging` nell'output indica `true`.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
```

```
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Creazione di percorso basato su una singola Regione

Il comando seguente crea un percorso basato su una singola Regione. Il bucket Amazon S3 specificato deve già esistere e avere le autorizzazioni appropriate CloudTrail applicate. Per ulteriori informazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket
```

Di seguito è riportato un output di esempio.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Creazione di un percorso multiregionale con la convalida dei file di registro abilitata

Per abilitare la convalida dei file di log quando usi `create-trail`, usa l'opzione `--enable-log-file-validation`.

Per informazioni sulla convalida dei file di log, consulta Convalida dell'integrità dei file di CloudTrail registro.

L'esempio seguente crea un percorso multiregionale che consegna i log al bucket specificato. Il comando utilizza l'opzione `--enable-log-file-validation`.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
multi-region-trail --enable-log-file-validation
```

A conferma che la convalida dei file di log è abilitata, l'elemento `LogFileValidationEnabled` nell'output indica `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Utilizzo del **`update-trail`** comando per aggiornare un trail

> **Important**
>
> A partire dal 22 novembre 2021, è AWS CloudTrail cambiato il modo in cui i trail registrano gli eventi di servizio globale. Ora, gli eventi creati da Amazon CloudFront AWS STS vengono registrati nella regione in cui sono stati creati, la regione Stati Uniti orientali (Virginia settentrionale), us-east-1. AWS Identity and Access Management In questo modo il modo in cui vengono CloudTrail trattati questi servizi è coerente con quello di altri servizi globali. AWS Per continuare a ricevere eventi di assistenza globale al di fuori della regione Stati Uniti orientali (Virginia settentrionale), assicurati di convertire i percorsi a Regione singola che utilizzano eventi di assistenza globale al di fuori di Stati Uniti orientali (Virginia settentrionale) in percorsi multi-regione. Per ulteriori informazioni sull'acquisizione di eventi di assistenza globale, consulta Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale più avanti in questa sezione.
> Al contrario, la cronologia degli eventi nella CloudTrail console e il aws cloudtrail lookup-events comando mostreranno questi eventi nel luogo in Regione AWS cui si sono verificati.

Puoi utilizzare il comando `update-trail` per modificare le impostazioni di configurazione per un trail. È inoltre possibile utilizzare i comandi remove-tags e add-tags per aggiungere e rimuovere i tag per un trail. Puoi aggiornare solo i percorsi della AWS regione in cui è stato creato il percorso (la sua regione d'origine). Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella AWS regione configurata per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Se hai abilitato gli eventi di CloudTrail gestione in Amazon Security Lake, devi mantenere almeno un percorso organizzativo multiregionale e registrare sia `read` gli eventi che gli eventi di `write` gestione. Non puoi aggiornare un percorso qualificante in modo che non soddisfi i requisiti di Security Lake. Ad esempio, modificando il percorso in Regione singola o disattivando la registrazione degli eventi di gestione `read` o `write`.

> **Note**
>
> Se usi il AWS CLI o uno dei due AWS SDKs per modificare un percorso, assicurati che la policy del bucket del percorso sia quella corretta. up-to-date Affinché il tuo bucket riceva automaticamente eventi da un nuovo utente Regione AWS, la policy deve contenere il nome completo del servizio,. `cloudtrail.amazonaws.com` Per ulteriori informazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.

Argomenti

- Conversione di un percorso a regione singola in un percorso multiregionale
- Conversione di un percorso multi-regione in un percorso basato su una Regione singola
- Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale
- Abilitazione della convalida dei file di log
- Disabilitazione della convalida dei file di log

Conversione di un percorso a regione singola in un percorso multiregionale

Per modificare un itinerario a regione singola esistente in un percorso multiregionale, usa l'opzione. `--is-multi-region-trail`

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Per confermare che il percorso è ora un percorso multiregionale, verificate che l'`IsMultiRegionTrail`elemento nell'output sia visualizzato. `true`

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
```

```
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Conversione di un percorso multi-regione in un percorso basato su una Regione singola

Per modificare un percorso multi-regione esistente in modo che si applichi solo alla Regione in cui è stato creato, utilizza l'opzione `--no-is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

A conferma che il trail è valido per una singola regione, l'elemento `IsMultiRegionTrail` nell'output indica `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Abilitazione e disabilitazione della registrazione degli eventi di assistenza globale

Per modificare un trail in modo che non registri gli eventi di servizio globali, utilizza l'opzione `--no-include-global-service-events`.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

A conferma che il trail non registra più gli eventi di servizio globali, l'elemento `IncludeGlobalServiceEvents` nell'output indica `false`.

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
```

```
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Per modificare un trail in modo che registri gli eventi di servizio globali, utilizza l'opzione `--include-global-service-events`.

I percorsi a Regione singola non riceveranno più eventi di assistenza globale a partire dal 22 novembre 2021, a meno che il percorso non compaia già nella Regione Stati Uniti orientali (Virginia settentrionale), us-east-1. Per continuare ad acquisire eventi di servizio globale, aggiorna la configurazione del percorso in un percorso multi-regione. Ad esempio, questo comando aggiorna un percorso basato su una singola Regione negli Stati Uniti orientali (Ohio) us-east-2, in un percorso multi-regione. *`myExistingSingleRegionTrailWithGSE`*Sostituiscilo con il nome del percorso appropriato per la tua configurazione.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Poiché gli eventi di assistenza globale sono disponibili solo negli Stati Uniti orientali (Virginia settentrionale) dal 22 novembre 2021, puoi anche creare un percorso a una sola Regione per iscriverti agli eventi di assistenza globali nella Regione Stati Uniti orientali (Virginia settentrionale), us-east-1. Il comando seguente crea un percorso a regione singola in us-east-1 per CloudFront ricevere, IAM ed eventi: AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name amzn-s3-demo-bucket
```

Abilitazione della convalida dei file di log

Per abilitare la convalida dei file di log per un trail, usa l'opzione `--enable-log-file-validation`. I file digest vengono distribuiti nel bucket Amazon S3 per il percorso specificato.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

A conferma che la convalida dei file di log è abilitata, l'elemento `LogFileValidationEnabled` nell'output indica `true`.

```
{
    "IncludeGlobalServiceEvents": true,
```

```
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Disabilitazione della convalida dei file di log

Per disabilitare la convalida dei file di log per un trail, usa l'opzione `--no-enable-log-file-validation`.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

A conferma che la convalida dei file di log è disabilitata, l'elemento `LogFileValidationEnabled` nell'output indica `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Per convalidare i file di registro con, vedere. AWS CLIConvalida dell'integrità dei file di CloudTrail registro con AWS CLI

Gestire i percorsi con AWS CLI

AWS CLI Include diversi altri comandi che ti aiutano a gestire i tuoi percorsi. Questi comandi aggiungere i tag ai trail, ne ottengono lo stato, ne avviano e ne arrestano la registrazione e li eliminano. È necessario eseguire questi comandi dalla stessa AWS regione in cui è stato creato il percorso (la sua regione di origine). Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella AWS regione configurata per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro --region con il comando.

Argomenti

- Aggiungere uno o più tag a un trail
- Elencare i tag per uno o più trail
- Rimuovere uno o più tag da un trail
- Recupero delle impostazioni e dello stato di un trail
- Configurazione dei selettori CloudTrail di eventi di Insights
- Configurazione di selettori di eventi avanzati
- Configurazione dei selettori di eventi di base
- Arresto e avvio della registrazione di log per un trail
- Eliminazione di un trail

Aggiungere uno o più tag a un trail

Per aggiungere uno o più tag a un percorso esistente, esegui il comando add-tags.

L'esempio seguente aggiunge un tag con il nome *Owner* e il valore di *Mary* a un percorso con l'ARN di *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* nella regione Stati Uniti orientali (Ohio).

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

In caso di successo, questo comando non restituisce alcun risultato.

Elencare i tag per uno o più trail

Per visualizzare i tag associati a uno o più trail esistenti, utilizzare il comando list-tags.

L'esempio seguente elenca i tag per *Trail1* e. *Trail2*

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente.

```
{
 "ResourceTagList": [
     {
```

```
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
        "TagsList": [
            {
                "Value": "Alice",
                "Key": "Name"
            },
            {
                "Value": "Ohio",
                "Key": "Location"
            }
        ]
    },
    {
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
        "TagsList": [
            {
                "Value": "Bob",
                "Key": "Name"
            }
        ]
    }
  ]
}
```

Rimuovere uno o più tag da un trail

Per rimuovere uno o più tag da un percorso esistente, esegui il comando remove-tags.

L'esempio seguente rimuove i tag con i nomi `Location` e `Name` da un percorso con l'ARN della `arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1` regione Stati Uniti orientali (Ohio).

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

In caso di successo, questo comando non restituisce alcun risultato.

Recupero delle impostazioni e dello stato di un trail

Esegui il `describe-trails` comando per recuperare informazioni sui percorsi in una regione. AWS L'esempio seguente restituisce informazioni sui percorsi configurati nella regione Stati Uniti orientali (Ohio).

```
aws cloudtrail describe-trails --region us-east-2
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "amzn-s3-demo-bucket1",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "amzn-s3-demo-bucket2",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "amzn-s3-demo-bucket3",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
```

```
    }
  ]
}
```

Esegui il comando `get-trail` per recuperare le informazioni sulle impostazioni relative a un percorso specifico. L'esempio seguente restituisce le informazioni sulle impostazioni per un percorso denominato*my-trail*.

```
aws cloudtrail get-trail - -name my-trail
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente.

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "amzn-s3-demo-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

Esegui il comando `get-trail-status` per recuperare lo stato di un trail. È necessario eseguire questo comando dalla AWS regione in cui è stato creato (Home Region) oppure è necessario specificare tale regione aggiungendo il --region parametro.

> **Note**
>
> Se il percorso è un percorso organizzativo e tu sei un account membro dell'organizzazione in AWS Organizations, devi fornire l'ARN completo di quel percorso e non solo il nome.

```
aws cloudtrail get-trail-status --name my-trail
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Oltre ai campi visualizzati nel precedente codice JSON, lo stato contiene i seguenti campi se sono presenti errori di Amazon SNS o Amazon S3:

- `LatestNotificationError`. Contiene l'errore generato da Amazon SNS se una sottoscrizione a un argomento ha esito negativo.
- `LatestDeliveryError`. Contiene l'errore emesso da Amazon S3 CloudTrail se non è possibile inviare un file di registro a un bucket.

Configurazione dei selettori CloudTrail di eventi di Insights

Abilita gli eventi Insights su un trail eseguendo il comando put-insight-selectors e specificando `ApiCallRateInsight`, `ApiErrorRateInsight` o entrambi come valore dell'attributo `InsightType`. Per visualizzare le impostazioni dei selettori di eventi Insights per un trail, esegui il comando `get-insight-selectors`. È necessario eseguire questo comando dalla AWS regione in cui è stato creato il percorso (la Home Region) oppure è necessario specificare tale regione aggiungendo il --region parametro al comando.

> **Note**
>
> Per registrare gli eventi di Insights per `ApiCallRateInsight`, il percorso deve registrare gli eventi di gestione `write`. Per registrare gli eventi di Insights per `ApiErrorRateInsight`, il percorso deve registrare gli eventi di gestione `read` o `write`.

Percorso di esempio che registra gli eventi Insights

L'esempio seguente utilizza put-insight-selectors per creare un selettore di eventi Insights per un percorso denominato*TrailName3*. Ciò abilita la raccolta di eventi Insights per il *TrailName3* percorso. Il selettore eventi Insights registra entrambi i tipi di eventi Insights `ApiErrorRateInsight` e `ApiCallRateInsight`.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

L'esempio restituisce il selettore di eventi Insights configurato per il trail.

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Esempio: disattivazione della raccolta di eventi Insights

L'esempio seguente utilizza put-insight-selectors per rimuovere il selettore di eventi Insights per un percorso denominato*TrailName3*. La cancellazione della stringa JSON dei selettori di Insights disattiva la raccolta di eventi Insights per il percorso. *TrailName3*

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

Nell'esempio viene restituito il selettore, ora vuoto, di eventi Insights configurato per il trail.

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Configurazione di selettori di eventi avanzati

È possibile utilizzare selettori di eventi avanzati per registrare gli eventi di gestione, gli eventi relativi ai dati per tutti i tipi di risorse e gli eventi di attività di rete. Al contrario, è possibile utilizzare selettori di eventi di base per registrare gli eventi di gestione e gli eventi relativi ai dati per i `AWS::DynamoDB::Table` tipi `AWS::Lambda::Function` di `AWS::S3::Object` risorse e. È possibile utilizzare selettori di eventi di base o selettori di eventi avanzati, ma non entrambi. Se si applicano selettori di eventi avanzati a un percorso che utilizza selettori di eventi di base, i selettori di eventi di base vengono sovrascritti.

Per convertire un itinerario in selettori di eventi avanzati, esegui il get-event-selectors comando per confermare i selettori di eventi correnti, quindi configura i selettori di eventi avanzati in modo che corrispondano alla copertura dei selettori di eventi precedenti, quindi aggiungi eventuali selettori aggiuntivi.

È necessario eseguire il `get-event-selectors` comando dal Regione AWS punto in cui è stato creato il percorso (la Home Region) oppure specificare tale regione aggiungendo il parametro. --region

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Se il percorso è un percorso organizzativo e hai effettuato l'accesso con un account membro dell'organizzazione in AWS Organizations, devi fornire l'ARN completo del percorso e non solo il nome.

L'esempio seguente mostra le impostazioni di un percorso che utilizza selettori di eventi avanzati per registrare gli eventi di gestione. Per impostazione predefinita, un trail è configurato per registrare tutti gli eventi di gestione e nessun evento relativo ai dati o alle attività di rete.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events-
trail",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
```

```
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]

        }
    ]
}
```

Per creare un selettore di eventi avanzato, esegui il comando `put-event-selectors`. Quando si verifica un evento nel tuo account, CloudTrail valuta la configurazione dei tuoi percorsi. Se l'evento corrisponde a un qualsiasi selettore di eventi avanzato di un percorso, il percorso elabora e registra l'evento. Puoi configurare fino a 500 condizioni su un percorso, inclusi tutti i valori specificati per tutti i selettori di eventi avanzati sul percorso. Per ulteriori informazioni, consulta Registrazione degli eventi di dati e Registrazione degli eventi delle attività di rete.

Argomenti

- Percorso di esempio con selettori di eventi avanzati specifici
- Esempio di percorso che utilizza selettori di eventi avanzati personalizzati per registrare Amazon S3 AWS Outposts su eventi relativi ai dati
- Esempio di percorso che utilizza selettori di eventi avanzati per escludere gli eventi AWS Key Management Service
- Esempio di percorso che utilizza selettori di eventi avanzati per escludere gli eventi di gestione di Amazon RDS Data API

Percorso di esempio con selettori di eventi avanzati specifici

L'esempio seguente crea selettori di eventi avanzati personalizzati per un percorso denominato in *`TrailName`* modo da includere eventi di gestione di lettura e scrittura (omettendo il `readOnly` selettore) `PutObject` ed eventi di `DeleteObject` dati per tutte le combinazioni di bucket/prefisso Amazon S3 ad eccezione di un bucket denominato`amzn-s3-demo-bucket`, eventi di dati per una AWS Lambda funzione `MyLambdaFunction` denominata ed eventi di attività di rete per eventi ad accesso negato su un endpoint VPC. AWS KMS Poiché si tratta di selettori di eventi avanzati personalizzati, ogni set di selettori ha un nome descrittivo. Nota che una barra finale fa parte del valore ARN per i bucket S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  },
  {
     "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
     "FieldSelectors": [
       { "Field": "eventCategory", "Equals": ["NetworkActivity"]},
       { "Field": "eventSource", "Equals": ["kms.amazonaws.com"]},
       { "Field": "errorCode", "Equals": ["VpceAccessDenied"]}
     ]
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
```

```
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::amzn-s3-demo-bucket/" ]
        },
      ]
    },
    {
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:123456789012:function/
MyLambdaFunction" ]
        }
```

```
      ]
    },
    {
       "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
       "FieldSelectors": [
         {
           "Field": "eventCategory",
           "Equals": ["NetworkActivity"]
         },
         {
           "Field": "eventSource",
           "Equals": ["kms.amazonaws.com"]
         },
         {
           "Field": "errorCode",
           "Equals": ["VpceAccessDenied"]
         }
       ]
     }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Esempio di percorso che utilizza selettori di eventi avanzati personalizzati per registrare Amazon S3 AWS Outposts su eventi relativi ai dati

L'esempio seguente mostra come configurare il percorso per includere tutti gli eventi relativi ai dati per tutti gli Amazon S3 sugli AWS Outposts oggetti del tuo avamposto. In questa versione, il valore supportato per S3 sugli AWS Outposts eventi per il `resources.type` campo è. `AWS::S3Outposts::Object`

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

Esempio di percorso che utilizza selettori di eventi avanzati per escludere gli eventi AWS Key Management Service

L'esempio seguente crea un selettore di eventi avanzato per un percorso denominato *TrailName* per includere eventi di gestione di sola lettura e sola scrittura (omettendo il `readOnly` selettore), ma per escludere eventi (). AWS Key Management Service AWS KMS Poiché AWS KMS gli eventi vengono trattati come eventi gestionali e il loro volume può essere elevato, possono avere un impatto sostanziale sulla CloudTrail fattura se si dispone di più di un percorso che raccoglie gli eventi di gestione.

Se si sceglie di non registrare gli eventi di gestione, gli AWS KMS eventi non vengono registrati e non è possibile modificare le impostazioni di registrazione AWS KMS degli eventi.

Per ricominciare a registrare AWS KMS gli eventi in un percorso, rimuovete il `eventSource` selettore ed eseguite nuovamente il comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
```

```
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per avviare nuovamente la registrazione di eventi su un percorso, rimuovi il selettore `eventSource`, come mostrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
```

```
  }
]'
```

Esempio di percorso che utilizza selettori di eventi avanzati per escludere gli eventi di gestione di Amazon RDS Data API

L'esempio seguente crea un selettore di eventi avanzato per un percorso denominato *TrailName* per includere eventi di gestione di sola lettura e sola scrittura (omettendo il `readOnly` selettore), ma per escludere gli eventi di gestione delle API di Amazon RDS Data. Per escludere gli eventi di gestione di Amazon RDS Data API, specifica l'origine dell'evento Amazon RDS Data API nel valore della stringa per il `eventSource` campo:. `rdsdata.amazonaws.com`

Se scegli di non registrare gli eventi di gestione, gli eventi di gestione di Amazon RDS Data API non vengono registrati e non puoi modificare le impostazioni di registrazione degli eventi di Amazon RDS Data API.

Per ricominciare a registrare gli eventi di gestione delle API di Amazon RDS Data su un trail, rimuovi il `eventSource` selettore ed esegui nuovamente il comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
```

```
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per avviare nuovamente la registrazione di eventi su un percorso, rimuovi il selettore `eventSource`, come mostrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Configurazione dei selettori di eventi di base

È possibile utilizzare solo i selettori di eventi di base per registrare gli eventi di gestione e gli eventi relativi ai dati per i tipi `AWS::DynamoDB::Table` di risorse e`AWS::S3::Object`. `AWS::Lambda::Function` È possibile registrare gli eventi di gestione, tutti i tipi di risorse dati e gli eventi di attività di rete utilizzando selettori di eventi avanzati.

È possibile utilizzare selettori di eventi di base o selettori di eventi avanzati, ma non entrambi. Se si applicano selettori di eventi di base a un percorso che utilizza selettori di eventi avanzati, i selettori di eventi avanzati vengono sovrascritti.

Per visualizzare le impostazioni dei selettori di eventi per un trail, esegui il comando `get-event-selectors`. È necessario eseguire questo comando dal Regione AWS punto in cui è stato creato (la Home Region) oppure è necessario specificare tale regione utilizzando il parametro. --region

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Se il percorso è un percorso organizzativo e tu sei un account membro dell'organizzazione in AWS Organizations, devi fornire l'ARN completo di quel percorso e non solo il nome.

L'esempio seguente mostra le impostazioni di un percorso che utilizza selettori di eventi di base per registrare gli eventi di gestione.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per creare un selettore di eventi, esegui il comando `put-event-selectors`. Se desideri registrare gli eventi di Insights sul percorso, assicurati che il selettore di eventi consenta la registrazione dei tipi di Insights per i quali desideri configurare il percorso. Per ulteriori informazioni sulla registrazione di eventi Insights, consulta Lavorare con CloudTrail Insights.

Quando si verifica un evento nel tuo account, CloudTrail valuta la configurazione del trail. Se l'evento corrisponde a un qualsiasi selettore di eventi di un trail, il trail elabora e registra l'evento. Per un trail puoi configurare fino a 5 selettori di eventi e un massimo di 250 risorse di dati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.

Argomenti

- Percorso di esempio con selettori di eventi specifici
- Percorso di esempio che registra tutti gli eventi di gestione e di dati
- Esempio di percorso che non registra AWS Key Management Service gli eventi
- Esempio di percorso che registra gli eventi rilevanti a basso volume AWS Key Management Service
- Percorso di esempio che non registra gli eventi dell'API dati di Amazon RDS

Percorso di esempio con selettori di eventi specifici

L'esempio seguente crea un selettore di eventi per un percorso denominato in *TrailName* modo da includere eventi di gestione di sola lettura e sola scrittura, eventi di dati per due combinazioni di bucket/prefisso Amazon S3 ed eventi di dati per una singola funzione denominata. AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-
demo-bucket/prefix","arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"]},
{"Type": "AWS::Lambda::Function","Values": ["arn:aws:lambda:us-
west-2:999999999999:function:hello-world-python-function"]}]}]'
```

L'esempio restituisce il selettore di eventi configurato per il trail.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Percorso di esempio che registra tutti gli eventi di gestione e di dati

L'esempio seguente crea un selettore di eventi per un percorso denominato *TrailName2* che include tutti gli eventi di gestione, inclusi gli eventi di gestione di sola lettura e di sola scrittura, e gli eventi di dati per tutti i bucket, le funzioni AWS Lambda e le tabelle Amazon DynamoDB di Amazon S3 in. Account AWS Poiché questo esempio utilizza selettori di eventi di base, non può configurare la registrazione per gli eventi S3 AWS Outposts, le chiamate JSON-RPC di Amazon Managed Blockchain sui nodi Ethereum o altri tipi di risorse di selezione di eventi avanzati. Inoltre, non puoi registrare gli eventi di attività di rete utilizzando selettori di eventi di base. È necessario utilizzare selettori di eventi avanzati per registrare gli eventi di attività di rete e gli eventi relativi ai dati per tutti gli altri tipi di risorse. Per ulteriori informazioni, consulta Configurazione di selettori di eventi avanzati.

> **Note**
>
> Se il percorso è valido solo per una regione, vengono registrati solo gli eventi in tale regione, anche se i parametri del selettore di eventi specificano tutti i bucket Amazon S3 e le funzioni Lambda. I selettori di eventi sono validi per le regioni in cui il trail è stato creato.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

L'esempio restituisce i selettori di eventi configurati per il trail.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
```

```
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Esempio di percorso che non registra AWS Key Management Service gli eventi

L'esempio seguente crea un selettore di eventi per un trail denominato in *`TrailName`* modo da includere eventi di gestione di sola lettura e sola scrittura, ma per escludere gli eventi (). AWS Key Management Service AWS KMS Poiché AWS KMS gli eventi vengono trattati come eventi di gestione e il loro volume può essere elevato, possono avere un impatto sostanziale sulla CloudTrail fattura se si dispone di più di un percorso che raccoglie gli eventi di gestione. L'utente in questo esempio ha scelto di escludere gli eventi AWS KMS da tutti i trail tranne uno. Per escludere un'origine evento, aggiungere `ExcludeManagementEventSources` ai selettori di eventi e specificare un'origine evento nel valore stringa.

Se si sceglie di non registrare gli eventi di gestione, gli AWS KMS eventi non vengono registrati e non è possibile modificare le impostazioni di registrazione AWS KMS degli eventi.

Per ricominciare a registrare AWS KMS gli eventi su un percorso, passate un array vuoto come valore di. `ExcludeManagementEventSources`

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

Nell'esempio viene restituito il selettore di eventi configurato per il trail.

```
{
```

```
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per ricominciare a registrare AWS KMS gli eventi su un percorso, passate un array vuoto come valore di`ExcludeManagementEventSources`, come illustrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Esempio di percorso che registra gli eventi rilevanti a basso volume AWS Key Management Service

L'esempio seguente crea un selettore di eventi per un percorso denominato in *`TrailName`* modo da includere eventi ed eventi di gestione di sola scrittura. AWS KMS Poiché AWS KMS gli eventi vengono trattati come eventi gestionali e il loro volume può essere elevato, possono avere un impatto sostanziale sulla CloudTrail fattura se si dispone di più di un percorso che raccoglie gli eventi di gestione. L'utente in questo esempio ha scelto di includere gli eventi AWS KMS Write, che includeranno `Delete` e `DisableScheduleKey`, ma non includeranno più azioni ad alto volume come `EncryptDecrypt`, e `GenerateDataKey` (questi ora vengono considerati come eventi di lettura).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Nell'esempio viene restituito il selettore di eventi configurato per il trail. In questo modo vengono registrati gli eventi di gestione di sola scrittura, inclusi gli eventi. AWS KMS

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
```

```
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Percorso di esempio che non registra gli eventi dell'API dati di Amazon RDS

L'esempio seguente crea un selettore di eventi per un percorso denominato *TrailName* per includere eventi di gestione di sola lettura e sola scrittura, ma per escludere gli eventi Amazon RDS Data API. Poiché gli eventi di Amazon RDS Data API vengono trattati come eventi di gestione e possono essercene un volume elevato, possono avere un impatto sostanziale sulla CloudTrail bolletta se disponi di più di un percorso che registra gli eventi di gestione. L'utente in questo esempio ha scelto di escludere gli eventi dell'API dati di Amazon RDS da tutti i percorsi, tranne uno. Per escludere un'origine eventi, aggiungi `ExcludeManagementEventSources` ai selettori di eventi e specifica l'origine eventi dell'API dati di Amazon RDS nel valore della stringa: `rdsdata.amazonaws.com`.

Se scegli di non registrare gli eventi di gestione, gli eventi dell'API dati di Amazon RDS non vengono registrati e non puoi modificare le impostazioni di registrazione degli eventi.

Per ricominciare a registrare gli eventi di gestione delle API di Amazon RDS Data su un trail, passa un array vuoto come valore di. `ExcludeManagementEventSources`

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

Nell'esempio viene restituito il selettore di eventi configurato per il trail.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
```

```
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per ricominciare a registrare gli eventi di gestione delle API di Amazon RDS Data su un trail, passa un array vuoto come valore di`ExcludeManagementEventSources`, come mostrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Arresto e avvio della registrazione di log per un trail

I seguenti comandi avviano e CloudTrail interrompono la registrazione.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> Prima di eliminare un bucket, esegui il comando `stop-logging` per interrompere la distribuzione degli eventi nel bucket. Se non interrompi la registrazione, CloudTrail tenta di inviare i file di registro a un bucket con lo stesso nome per un periodo di tempo limitato.
> Se interrompi la registrazione o elimini un percorso, CloudTrail Insights viene disabilitato su quel percorso.

Eliminazione di un trail

Se hai abilitato gli eventi di CloudTrail gestione in Amazon Security Lake, devi mantenere almeno un percorso organizzativo multiregionale e registrare sia `read` gli eventi che gli eventi di `write` gestione. Non puoi eliminare un trail se è l'unico a tua disposizione che soddisfa questo requisito, a meno che non disattivi gli eventi di CloudTrail gestione in Security Lake.

Puoi eliminare un trail con il comando seguente. Puoi eliminare un trail solo nella regione in cui è stato creato (la regione principale).

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Quando elimini un percorso, non elimini il bucket Amazon S3 o l'argomento Amazon SNS associato ad esso. Utilizza l'API AWS Management Console AWS CLI, o service per eliminare queste risorse separatamente.

Creazione di percorsi multipli

Puoi utilizzare i file di CloudTrail registro per risolvere problemi operativi o di sicurezza del tuo AWS account. Puoi creare trail per diversi utenti, che a loro volta potranno e gestire i propri trail. Puoi configurare trail per distribuire i file di log in bucket S3 diversi o in bucket S3 condivisi.

> **Note**
>
> La prima copia degli eventi di gestione di Regione AWS ciascun account è gratuita. Se crei più percorsi che consegnano gli stessi eventi di gestione ad altre destinazioni, tali consegne successive comportano dei costi CloudTrail . Per ulteriori informazioni sui CloudTrail costi, consulta AWS CloudTrail Prezzi e. Gestione dei costi dei CloudTrail percorsi

In uno scenario di esempio potrebbero essere presenti i seguenti utenti:

- Un amministratore della sicurezza crea un percorso nella regione Europa (Irlanda) e configura la crittografia KMS dei file di log. Il percorso distribuisce i file di log in un bucket S3 nella regione Europa (Irlanda).
- Un revisore IT crea un percorso nella regione Europa (Irlanda) e configura la convalida dell'integrità dei file di registro per garantire che i file di registro non siano cambiati da quando sono stati consegnati. CloudTrail Il percorso è configurato per distribuire i file di log in un bucket S3 nella regione Europa (Francoforte)
- Uno sviluppatore crea un percorso nella regione Europa (Francoforte) e configura gli CloudWatch allarmi per ricevere notifiche per attività API specifiche. Il trail condivide lo stesso bucket S3 del trail configurato per l'integrità dei file di log.
- Un altro sviluppatore crea un percorso nella regione Europa (Francoforte) e configura SNS. I file di log vengono distribuiti in un bucket S3 separato nella regione Europa (Francoforte).

Nell'immagine seguente viene descritto questo esempio.

> **Note**
>
> Puoi creare fino a cinque percorsi per. Regione AWS Un percorso multiregionale conta come un percorso per regione.

Puoi utilizzare le autorizzazioni a livello di risorsa per gestire la capacità di un utente per eseguire operazioni specifiche su CloudTrail.

Ad esempio, puoi concedere a un utente l'autorizzazione di visualizzare le attività dei trail, ma impedirgli di avviare o interrompere la registrazione dei log per un trail. Puoi concedere un altro utente l'autorizzazione completa per creare ed eliminare i trail. Ciò garantisce un controllo su trail e accesso utenti a un livello più granulare.

Per ulteriori informazioni sulle autorizzazioni a livello di risorsa, consulta Esempi: creazione e applicazione di policy per le operazioni su percorsi specifici.

Per ulteriori informazioni su più percorsi, vedere il CloudTrail FAQs.

Creazione di un percorso per un'organizzazione

Se hai creato un'organizzazione in AWS Organizations, puoi creare un percorso che registri tutti Account AWS gli eventi di quell'organizzazione. Questa soluzione viene talvolta chiamata percorso dell'organizzazione.

L'account di gestione dell'organizzazione può assegnare un amministratore delegato per creare nuovi percorsi organizzativi o gestire i percorsi organizzativi esistenti. Per ulteriori informazioni sull'aggiunta di un amministratore delegato, consulta Aggiunta di un CloudTrail amministratore delegato.

L'account di gestione dell'organizzazione può modificare un percorso esistente nel proprio account e applicarlo a un'organizzazione, trasformandolo in un percorso dell'organizzazione. I percorsi dell'organizzazione registrano eventi per l'account di gestione e per tutti gli account membri dell'organizzazione. Per ulteriori informazioni su AWS Organizations, vedere Organizations Terminology and Concepts.

> **Note**
>
> Per creare un percorso dell'organizzazione, devi effettuare l'accesso con l'account di gestione o con l'account dell'amministratore delegato dell'organizzazione. È inoltre necessario disporre di autorizzazioni sufficienti per consentire all'utente o al ruolo nell'account di gestione o

amministratore delegato di creare il percorso. Se non disponi di autorizzazioni sufficienti, non avrai l'opzione per applicare il percorso a un'organizzazione.

Tutti gli itinerari organizzativi creati utilizzando la console sono percorsi organizzativi multiregionali che registrano gli eventi dagli account abilitati Regioni AWS in ogni membro dell'organizzazione. Per registrare gli eventi in tutte le AWS partizioni dell'organizzazione, crea un itinerario organizzativo multiregionale in ogni partizione. È possibile creare un itinerario organizzativo a regione singola o multiarea utilizzando. AWS CLI Se si crea un itinerario a regione singola, si registra l'attività solo nel percorso Regione AWS (noto anche come regione principale).

Sebbene la Regioni AWS maggior parte sia abilitata di default per la tua Account AWS, devi abilitare manualmente alcune regioni (chiamate anche regioni opzionali). Per informazioni su quali regioni sono abilitate per impostazione predefinita, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Gestione dell'account AWS Guida di riferimento. Per l'elenco delle regioni CloudTrail supportate, vedere. CloudTrail Regioni supportate

Quando crei un percorso organizzativo, una copia del percorso con il nome che gli hai assegnato viene creata negli account dei membri che appartengono alla tua organizzazione.

- Se l'organigramma riguarda una singola regione e la regione di origine del percorso non è una regione che ha aderito, viene creata una copia del percorso nella regione di origine dell'organigramma in ogni account membro.
- Se l'organizzazione trail è per una regione singola e la regione di origine del percorso è una regione che ha aderito, una copia del percorso viene creata nella regione di origine dell'organizzazione negli account dei membri che hanno abilitato tale regione.
- Se il percorso organizzativo è multiregionale e la regione di origine del percorso non è una regione che accetta l'iscrizione, viene creata una copia del percorso in ogni account membro abilitato Regione AWS . Quando un account membro abilita una regione con iscrizione, una volta completata l'attivazione di tale regione, viene creata una copia del percorso multiregionale nella regione appena attivata per l'account membro.
- Se il percorso organizzativo è multiregionale e la regione di origine è una regione con attivazione, gli account dei membri non invieranno attività al percorso organizzativo a meno che non scelgano il luogo in Regione AWS cui è stato creato il percorso multiregionale. Ad esempio, se crei un percorso multiregionale e scegli la regione Europa (Spagna) come regione di origine del percorso, solo gli account dei membri che hanno abilitato la regione Europa (Spagna) per il proprio account invieranno l'attività dell'account all'organigramma.

> **Note**
>
> CloudTrail crea gli itinerari organizzativi negli account dei membri anche se la convalida di una risorsa fallisce. Alcuni esempi di errori di convalida includono:
>
> - una policy sui bucket Amazon S3 errata
> - una politica tematica di Amazon SNS errata
> - impossibilità di effettuare consegne a un gruppo di CloudWatch log di Logs
> - autorizzazione insufficiente per crittografare utilizzando una chiave KMS
>
> Un account membro con CloudTrail autorizzazioni può visualizzare eventuali errori di convalida di un percorso organizzativo visualizzando la pagina dei dettagli del percorso sulla CloudTrail console o eseguendo il comando. AWS CLI get-trail-status

Gli utenti con CloudTrail autorizzazioni negli account dei membri possono visualizzare gli itinerari organizzativi quando accedono alla CloudTrail console dal proprio Account AWS account o quando AWS CLI eseguono comandi come. `describe-trails` Tuttavia, gli utenti degli account membro non dispongono di autorizzazioni sufficienti per eliminare gli itinerari organizzativi, attivare o disattivare la connessione, modificare i tipi di eventi registrati o modificare in altro modo un organigramma.

Quando crei un organigramma nella console, CloudTrail crea un ruolo collegato al servizio per eseguire attività di registrazione negli account dei membri dell'organizzazione. Questo ruolo è denominato AWSServiceRoleForCloudTrailed è necessario per registrare gli eventi CloudTrail di un'organizzazione. Se Account AWS viene aggiunto un account a un'organizzazione, vengono aggiunti l'itinerario organizzativo e il ruolo collegato al servizio e la registrazione per quell' Account AWS account inizia automaticamente nell'organigramma. Se un utente Account AWS viene rimosso da un'organizzazione, l'organigramma e il ruolo collegato ai servizi vengono eliminati dall'organizzazione Account AWS che non fa più parte dell'organizzazione. Tuttavia, i file di log per l'account rimosso creati prima della rimozione dell'account rimangono comunque nel bucket Simple Storage Service (Amazon S3) in cui sono archiviati per il percorso.

Se l'account di gestione di un' AWS Organizations organizzazione crea un percorso organizzativo, ma poi viene rimosso come account di gestione dell'organizzazione, qualsiasi percorso organizzativo creato utilizzando il relativo account diventa un percorso non organizzativo.

Nell'esempio seguente, l'account di gestione dell'organizzazione 1111 crea un percorso denominato *MyOrganizationTrail* per l'organizzazione. *o-exampleorgid* Il percorso registra l'attività per tutti gli account dell'organizzazione nello stesso bucket Amazon S3. Tutti gli account dell'organizzazione possono visualizzare *MyOrganizationTrail* l'elenco dei percorsi, ma gli account dei membri non possono rimuovere o modificare l'itinerario dell'organizzazione. Solo l'account di gestione o l'account dell'amministratore delegato può modificare o eliminare il trail per l'organizzazione. Solo l'account di gestione può rimuovere un account membro da un'organizzazione. Analogamente, per impostazione predefinita, solo l'account di gestione ha accesso al bucket Amazon S3 per il percorso e ai log in esso contenuti. La struttura a bucket di alto livello per i file di registro contiene una cartella denominata con l'ID dell'organizzazione e sottocartelle denominate con l'account IDs per ogni account dell'organizzazione. Gli eventi per ogni account membro vengono registrati nella cartella corrispondente all'ID dell'account membro. Se l'account membro 444444444444 viene rimosso dall'organizzazione *MyOrganizationTrail* e il ruolo collegato al servizio non viene più visualizzato nell' AWS account 444444444444 e nessun altro evento viene registrato per quell'account dall'organigramma. Tuttavia, la cartella 444444444444 rimane nel bucket Amazon S3, con tutti i log creati prima della rimozione dell'account dall'organizzazione.

In questo esempio, l'ARN del percorso creato nell'account di gestione è `aws:cloudtrail:us-east-2:111111111111:trail/`*MyOrganizationTrail*. Questo ARN è l'ARN per il trail membro anche in tutti gli account membri.

I trail dell'organizzazione sono simili ai trail standard per molti aspetti. È possibile creare più percorsi per l'organizzazione e scegliere se creare un percorso organizzativo multiregionale o a regione singola e quali tipi di eventi si desidera registrare nel percorso organizzativo, proprio come in qualsiasi altro percorso. Tuttavia, non vi sono alcune differenze. Ad esempio, quando crei un trail nella console e scegli se registrare gli eventi relativi ai dati per i bucket o AWS Lambda le funzioni di Amazon S3, le uniche risorse elencate nella CloudTrail console sono quelle per l'account di gestione, ma puoi aggiungere le risorse ARNs for negli account dei membri. Gli eventi di dati per le risorse dell'account membro specificato vengono registrati senza dover configurare manualmente l'accesso di più account a tali risorse. Per ulteriori informazioni sulla registrazione degli eventi di gestione, degli eventi Insights e degli eventi relativi ai dati, consultaRegistrazione degli eventi di gestione, Registrazione degli eventi di dati e. Lavorare con CloudTrail Insights

> **Note**
>
> Nella console, crei un percorso multiregionale. Si consiglia di registrare le attività in tutte le regioni abilitate del proprio paese Account AWS, in quanto ciò consente di mantenere AWS l'ambiente più sicuro. Per creare un percorso a singola Regione, utilizza la AWS CLI.

Quando visualizzi gli eventi nella Cronologia degli eventi di un'organizzazione in AWS Organizations, puoi visualizzare gli eventi solo per l'utente Account AWS con cui hai effettuato l'accesso. Ad esempio, se hai effettuato l'accesso con l'account di gestione dell'organizzazione, Event history (Cronologia eventi) mostra gli ultimi 90 giorni di eventi di gestione per l'account di gestione. Gli eventi dell'account membro dell'organizzazione non sono visualizzati inEvent history (Cronologia eventi) per l'account di gestione. Per visualizzare gli eventi dell'account membro in Event history (Cronologia eventi), accedi con l'account membro.

È possibile configurare altri AWS servizi per analizzare ulteriormente i dati degli eventi raccolti nei CloudTrail registri di un percorso organizzativo e agire in base a tali dati, nello stesso modo in cui si farebbe per qualsiasi altro percorso. Ad esempio, puoi analizzare i dati in un percorso dell'organizzazione utilizzando Amazon Athena. Per ulteriori informazioni, consulta AWS integrazioni di servizi con registri CloudTrail .

Argomenti

- Passaggio dai percorsi degli account dei membri ai percorsi organizzativi
- Preparazione per la creazione di un percorso per la tua organizzazione
- Creazione di un percorso per la tua organizzazione nella console
- Creare un percorso per un'organizzazione con AWS CLI
- Risoluzione dei problemi relativi a un percorso organizzativo

Passaggio dai percorsi degli account dei membri ai percorsi organizzativi

Se disponi già di CloudTrail percorsi configurati per gli account dei singoli membri, ma desideri passare a un percorso organizzativo per registrare gli eventi in tutti gli account, non vuoi perdere gli eventi eliminando gli itinerari degli account dei singoli membri prima di creare un percorso organizzativo. Tuttavia quando hai due trail, i costi saranno più elevati a causa della copia aggiuntiva degli eventi distribuiti al trail dell'organizzazione.

Per semplificare la gestione dei costi evitando di perdere gli eventi prima che la distribuzione dei log inizi nel trail dell'organizzazione, è consigliabile mantenere i trail dei singoli account membro e il trail dell'organizzazione per un massimo di un giorno. Ciò garantisce che il trail dell'organizzazione registri tutti gli eventi, ma i costi degli eventi duplicati vengono conteggiati solo per un giorno. Dopo il primo giorno, puoi interrompere la registrazione (o eliminare) ogni trail dei singoli account membro.

Preparazione per la creazione di un percorso per la tua organizzazione

Prima di creare un trail per la tua organizzazione, assicurati che sia l'account di gestione dell'organizzazione che l'account di gestione siano configurati correttamente per la creazione di trail.

- La tua organizzazione deve disporre di tutte le caratteristiche abilitate prima di poter creare un trail. Per ulteriori informazioni, consulta Abilitazione di tutte le caratteristiche nell'organizzazione.
- L'account di gestione deve disporre del ruolo AWSServiceRoleForOrganizations. Questo ruolo viene creato automaticamente da Organizations al momento della creazione dell'organizzazione ed è necessario per CloudTrail registrare gli eventi di un'organizzazione. Per ulteriori informazioni, consulta Organizations e ruoli collegati ai servizi.
- L'utente o il ruolo che crea il percorso dell'organizzazione nell'account di gestione o nell'account dell'amministratore delegato deve disporre di autorizzazioni sufficienti per creare un percorso. È necessario almeno applicare la policy AWSCloudTrail_FullAccess, o una policy equivalente, a quel ruolo o utente. Devi inoltre disporre di autorizzazioni sufficienti in IAM e Organizations per creare il ruolo collegato al servizio e abilitare l'accesso sicuro. Se scegli di creare un nuovo bucket S3 per un percorso organizzativo utilizzando la console, CloudTrail la tua politica deve includere anche il `s3:PutEncryptionConfiguration` azione perché per impostazione predefinita la crittografia lato server è abilitata per il bucket. La policy di esempio seguente mostra le autorizzazioni minime richieste.

> **Note**
>
> Non dovresti condividere la AWSCloudTrail_FullAccesspolitica su larga scala tra i tuoi. Account AWS Dovresti invece limitarla agli Account AWS amministratori a causa della natura altamente sensibile delle informazioni raccolte da. CloudTrail Gli utenti con questo ruolo hanno la possibilità di disabilitare o riconfigurare le funzioni di auditing più sensibili e importanti negli Account AWS. Per questo motivo, l'accesso a questa policy deve essere strettamente controllato e monitorato.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- Per utilizzare AWS CLI o CloudTrail APIs per creare un percorso organizzativo, devi abilitare l'accesso affidabile per CloudTrail in Organizations e devi creare manualmente un bucket Amazon S3 con una politica che consenta la registrazione per un percorso organizzativo. Per ulteriori informazioni, consulta Creare un percorso per un'organizzazione con AWS CLI.
- Per utilizzare un ruolo IAM esistente per aggiungere il monitoraggio di un percorso organizzativo ad Amazon CloudWatch Logs, devi modificare manualmente il ruolo IAM per consentire la consegna dei CloudWatch log per gli account dei membri al gruppo CloudWatch Logs per l'account di gestione, come illustrato nell'esempio seguente.

> **Note**
>
> È necessario utilizzare un ruolo IAM e un gruppo di log CloudWatch Logs esistente nel proprio account. Non è possibile utilizzare un ruolo IAM o un gruppo di log CloudWatch Logs di proprietà di un account diverso.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",

                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Puoi saperne di più CloudTrail e CloudWatch accedere ad Amazon Logs. Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs Inoltre, considera i limiti imposti ai CloudWatch log e le considerazioni relative ai prezzi del servizio prima di decidere di abilitare l'esperienza per un'organizzazione. Per ulteriori informazioni, consulta CloudWatch Logs Limits e Amazon CloudWatch Pricing.

- Per registrare gli eventi relativi ai dati nella traccia della tua organizzazione per risorse specifiche negli account dei membri, prepara un elenco di Amazon Resource Names (ARNs) per ciascuna di queste risorse. Le risorse dell'account membro non vengono visualizzate nella CloudTrail console quando crei un percorso; puoi cercare le risorse nell'account di gestione su cui è supportata la raccolta di eventi di dati, come i bucket S3. Allo stesso modo, se desideri aggiungere risorse specifiche per i membri durante la creazione o l'aggiornamento di un percorso organizzativo dalla riga di comando, hai bisogno ARNs di tali risorse.

> **Note**
>
> Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per CloudTrail i prezzi, vedi AWS CloudTrail Prezzi.

Prima di creare un percorso organizzativo, dovresti anche prendere in considerazione la possibilità di verificare quanti percorsi esistono già nell'account di gestione e negli account dei membri. CloudTrail limita il numero di sentieri che possono essere creati in ogni regione. Non puoi superare questo limite nella Regione in cui crei il percorso dell'organizzazione nell'account di gestione. Tuttavia, il percorso verrà creato negli account membri anche se questi hanno raggiunto il limite di percorsi in una Regione. Il primo percorso degli eventi di gestione in qualsiasi Regione è gratuito, tuttavia si applicano tariffe per i percorsi aggiuntivi. Per ridurre il costo potenziale di un percorso dell'organizzazione, considera l'eliminazione di qualsiasi percorso non necessario negli account di gestione e membri. Per ulteriori informazioni sui CloudTrail prezzi, consulta la AWS CloudTrail pagina Prezzi.

Best practice relative alla sicurezza nei trail dell'organizzazione

Come best practice di sicurezza, consigliamo di aggiungere la chiave di condizione `aws:SourceArn` per i criteri delle risorse (come quelli per bucket S3, chiavi KMS o argomenti SNS) utilizzati con un trail dell'organizzazione. Il valore di `aws:SourceArn` è l'ARN del percorso organizzativo (o ARNs, se si utilizza la stessa risorsa per più di un itinerario, ad esempio lo stesso bucket S3 per archiviare i log di più di un percorso). Ciò garantisce che la risorsa, come un bucket S3, accetti solo i dati associati al trail specifico. L'ARN trail deve utilizzare l'ID account dell'account di gestione. Il seguente frammento di policy mostra un esempio in cui più di un trail utilizza la risorsa.

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
```

```
    }
}
```

Per informazioni su come aggiungere chiavi di condizione ai criteri delle risorse, consulta quanto segue:

- Policy sui bucket Amazon S3 per CloudTrail
- Configura le politiche AWS KMS chiave per CloudTrail
- Policy tematica di Amazon SNS per CloudTrail

Creazione di un percorso per la tua organizzazione nella console

Per creare un organigramma dalla CloudTrail console, è necessario accedere alla console come utente o ruolo nell'account di gestione o amministratore delegato con autorizzazioni sufficienti. Se non accedi con l'account di gestione o amministratore delegato, non vedrai l'opzione per applicare un percorso a un'organizzazione quando crei o modifichi un percorso dalla console. CloudTrail

Per creare un percorso organizzativo con AWS Management Console

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.

   Devi effettuare l'accesso come identità IAM nell'account di gestione o nell'account dell'amministratore delegato con autorizzazioni sufficienti per creare un percorso dell'organizzazione.
2. Scegliere Trails (Trail) e quindi Create trail (Crea trail).
3. Nella pagina Create Trail (Crea trail), in Trail name (Nome trail) digitare il nome del trail. Per ulteriori informazioni, consulta Requisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS.
4. Seleziona Enable for all accounts in my organization (Abilita per tutti gli account nella mia organizzazione). Puoi visualizzare questa opzione solo se hai effettuato l'accesso alla console con un utente o un ruolo nell'account di gestione o nell'account dell'amministratore delegato. Per creare un trail dell'organizzazione, è necessario assicurarsi che l'utente o il ruolo abbiano le autorizzazioni sufficienti.
5. Per Storage location (Posizione di storage), scegli Create new S3 bucket (Crea nuovo bucket S3) per creare un bucket. Quando crei un bucket, CloudTrail crea e applica le politiche del bucket richieste.

> **Note**
>
> Se scegli Use existing S3 bucket (Utilizza bucket S3 esistente), specifica un bucket in Trail log bucket name (Nome del bucket del log del percorso), oppure scegli Browse (Sfoglia) per scegliere un bucket. Puoi scegliere un bucket appartenente a qualsiasi account, tuttavia, la policy del bucket deve concedere l' CloudTrailautorizzazione alla scrittura su di esso. Per informazioni sulla modifica manuale della policy bucket, consulta Policy sui bucket Amazon S3 per CloudTrail.

Per facilitare la ricerca dei log, crea una nuova cartella (nota anche come prefisso) in un bucket esistente per archiviare i log. CloudTrail Inserire il prefisso in Prefix (Prefisso).

6. Per la crittografia SSE-KMS dei file di registro, scegli Abilitato se desideri crittografare i file di registro e i file digest utilizzando la crittografia SSE-KMS anziché la crittografia SSE-S3. L'impostazione predefinita è Enabled (Abilitata). Se non abiliti la crittografia SSE-KMS, i file di registro e i file digest vengono crittografati utilizzando la crittografia SSE-S3. Per ulteriori informazioni sulla crittografia SSE-KMS, consulta Utilizzo della crittografia lato server con AWS Key Management Service (SSE-KMS). Per ulteriori informazioni sulla crittografia SSE-S3, consulta Utilizzo della crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3).

   Se abiliti la crittografia SSE-KMS, scegli Nuova o Esistente. AWS KMS key In AWS KMS Alias, specifica un alias, nel formato. `alias/` *`MyAliasName`* Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console.

   > **Note**
   >
   > È anche possibile digitare l'ARN di una chiave da un altro account. Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. La politica chiave deve consentire di utilizzare la chiave CloudTrail per crittografare i file di registro e i file digest e consentire agli utenti specificati di leggere i file di registro o i file digest in formato non crittografato. Per informazioni sulla modifica manuale della policy della chiave, consulta Configura le politiche AWS KMS chiave per CloudTrail.

7. In Additional settings (Impostazioni aggiuntive) configura quanto segue.

a. In Enable log file validation (Abilita la convalida dei file di log), scegli Enabled (Abilitata) per attivare la distribuzione dei file digest di log nel bucket S3. È possibile utilizzare i file digest per verificare che i file di registro non siano stati modificati dopo la loro consegna. CloudTrail Per ulteriori informazioni, consulta Convalida dell'integrità dei file di CloudTrail registro.

b. Per la consegna delle notifiche SNS, scegli Abilitato per ricevere una notifica ogni volta che un log viene consegnato al tuo bucket. CloudTrail memorizza più eventi in un file di registro. Le notifiche SNS vengono inviate per ogni file di log, non per ogni evento. Per ulteriori informazioni, consulta Configurazione delle notifiche Amazon SNS per CloudTrail.

   Se abiliti le notifiche SNS, per Create a new SNS topic (Crea un nuovo argomento SNS) scegli New (Nuovo) per creare un argomento oppure scegli Existing (Esistente) per utilizzare un argomento esistente. Se si crea un percorso multiregionale, le notifiche SNS per le consegne di file di registro da tutte le regioni vengono inviate al singolo argomento SNS creato.

   Se scegli Nuovo, CloudTrail specifica automaticamente un nome per il nuovo argomento oppure puoi digitare un nome. Se scegli Existing (Esistente), seleziona un argomento SNS dall'elenco a discesa. È anche possibile immettere l'ARN di un argomento da un'altra regione o da un account con le autorizzazioni appropriate. Per ulteriori informazioni, consulta Policy tematica di Amazon SNS per CloudTrail.

   Se si crea un argomento, è necessario sottoscrivere l'argomento per ricevere le notifiche di distribuzione dei file di log. Puoi abilitare la sottoscrizione nella console Amazon SNS. Data la frequenza delle notifiche, ti consigliamo di configurare la sottoscrizione in modo da usare una coda Amazon SQS per gestire le notifiche a livello di programmazione. Per ulteriori informazioni, consulta Nozioni di base su Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

8. Facoltativamente, configura CloudTrail l'invio dei file di registro ai CloudWatch registri selezionando Abilitato nei registri. CloudWatch Per ulteriori informazioni, consulta Invio di eventi ai registri CloudWatch .

> **Note**
>
> Solo l'account di gestione può configurare un gruppo di log CloudWatch Logs per un percorso organizzativo utilizzando la console. L'amministratore delegato può configurare

un gruppo di log CloudWatch Logs utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API.

a. Se abiliti l'integrazione con CloudWatch Logs, scegli Nuovo per creare un nuovo gruppo di log o Esistente per utilizzarne uno esistente. Se scegli Nuovo, CloudTrail specifica automaticamente un nome per il nuovo gruppo di log oppure puoi digitare un nome.

b. Se scegli Existing (Esistente), seleziona un gruppo di log dall'elenco a discesa.

c. Scegli Nuovo per creare un nuovo ruolo IAM per le autorizzazioni di invio dei log ai Logs. CloudWatch Scegli Existing (Esistente) per selezionare un ruolo IAM esistente dall'elenco a discesa. L'istruzione della policy per il ruolo nuovo o esistente viene visualizzata quando espandi Policy document (Documento della policy). Per ulteriori informazioni su questo ruolo, consulta Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio.

> **Note**
>
> Durante la configurazione di un percorso, puoi scegliere un bucket S3 e un argomento SNS appartenenti a un altro account. Tuttavia, se desideri inviare eventi CloudTrail a un gruppo di log CloudWatch Logs, devi scegliere un gruppo di log esistente nel tuo account corrente.

9. Per i tag, puoi aggiungere fino a 50 coppie di chiavi di tag per aiutarti a identificare, ordinare e controllare l'accesso al tuo percorso. I tag possono aiutarti a identificare sia i CloudTrail percorsi che i bucket Amazon S3 che contengono CloudTrail i file di registro. È quindi possibile utilizzare i gruppi di risorse per le risorse CloudTrail . Per ulteriori informazioni, consultare AWS Resource Groups e Tag.

10. Nella pagina Choose log events (Seleziona eventi di log) seleziona i tipi di evento che vuoi registrare. Per Management events (Eventi di gestione), procedere nel seguente modo.

    a. Per API activity (Attività API), scegli se vuoi che il percorso registri eventi Read (Lettura), Write (Scrittura) o entrambi. Per ulteriori informazioni, consulta Eventi di gestione.

    b. Scegli Escludi AWS KMS eventi per filtrare AWS Key Management Service (AWS KMS) gli eventi dal tuo percorso. L'impostazione predefinita è includere tutti gli eventi AWS KMS .

    L'opzione per registrare o escludere AWS KMS gli eventi è disponibile solo se registri gli eventi di gestione sul percorso. Se si sceglie di non registrare gli eventi di gestione,

AWS KMS gli eventi non vengono registrati e non è possibile modificare le impostazioni di registrazione AWS KMS degli eventi.

AWS KMS azioni come `EncryptDecrypt`, e `GenerateDataKey` in genere generano un volume elevato (oltre il 99%) di eventi. Queste operazioni vengono ora registrate come eventi Read (Lettura). AWS KMS Le azioni pertinenti a basso volume come **`Disable`** e **`ScheduleKey`** (che in genere rappresentano meno dello 0,5% del volume degli AWS KMS eventi) vengono registrate come eventi di scrittura. **`Delete`**

Per escludere eventi a volume elevato come `Encrypt`, `Decrypt` e `GenerateDataKey`, ma registrare comunque eventi rilevanti come `Disable`, `Delete` e `ScheduleKey`, scegli di registrare gli eventi di gestione Write (Scrittura) e deseleziona la casella di controllo Exclude AWS KMS events (Escludi eventi KMS).

c. Scegli Exclude Amazon RDS Data API events (Escludi eventi dell'API dati di Amazon RDS) per escludere dal percorso gli eventi dell'API dati di Amazon Relational Database Service. L'impostazione predefinita è includere tutti gli eventi dell'API dati di Amazon RDS. Per ulteriori informazioni sugli eventi dell'API dati di Amazon RDS, consulta Registrazione delle chiamate dell'API dati con AWS CloudTrail nella Guida per l'utente di Amazon RDS per Aurora.

11. Per registrare gli eventi di dati, scegli Data events (Eventi di dati). Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

12.

> **Important**
>
> I passaggi 12-16 riguardano la configurazione degli eventi di dati tramite selettori di eventi avanzati, che sono l'impostazione predefinita. I selettori di eventi avanzati consentono di configurare più tipi di risorse e offrono un controllo dettagliato sugli eventi di dati acquisiti dal percorso. Se intendi registrare gli eventi di attività di rete, devi utilizzare selettori di eventi avanzati. Se si utilizzano selettori di eventi di base, completare i passaggi indicatiConfigurazione delle impostazioni degli eventi di dati utilizzando i selettori di eventi di base, quindi tornare al passaggio 17 di questa procedura.

Per Tipo di risorsa, scegliete il tipo di risorsa su cui desiderate registrare gli eventi relativi ai dati. Per ulteriori informazioni sui tipi di risorse disponibili, consultaEventi di dati.

13. Scegli un modello di selettore di registro. Puoi scegliere un modello predefinito o scegliere Personalizzato per definire le condizioni di raccolta degli eventi.

    Puoi scegliere tra i seguenti modelli predefiniti:

    - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
    - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
    - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
    - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
    - Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

    > **Note**
    >
    > La scelta di un modello predefinito per i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket attualmente presenti nel tuo AWS account e per tutti i bucket che crei dopo aver completato la creazione del trail. Consente inoltre la registrazione dell'attività relativa agli eventi relativi ai dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se tale attività viene eseguita su un bucket che appartiene a un altro account. AWS
    > Se il percorso è valido solo per una regione, la selezione di un modello predefinito che registra tutti i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non verranno registrati gli eventi di dati per i bucket Amazon S3 nelle altre regioni dell'account AWS .
    > Se stai creando un percorso multiregionale, la scelta di un modello predefinito per le funzioni Lambda abilita la registrazione degli eventi dei dati per tutte le funzioni attualmente presenti nel tuo AWS account e per tutte le funzioni Lambda che potresti creare in qualsiasi regione dopo aver completato la creazione del percorso. Se stai creando un percorso per una singola regione (eseguita utilizzando il AWS CLI), questa

selezione abilita la registrazione degli eventi di dati per tutte le funzioni attualmente presenti in quella regione nel tuo AWS account e per tutte le funzioni Lambda che potresti creare in quella regione dopo aver terminato la creazione del percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
La registrazione degli eventi relativi ai dati per tutte le funzioni consente inoltre di registrare l'attività degli eventi relativi ai dati eseguita da qualsiasi identità IAM nel tuo AWS account, anche se tale attività viene eseguita su una funzione che appartiene a un altro account. AWS

14. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
15. Se hai selezionato Personalizzato, in Advanced event selectors crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

a. Scegli tra i seguenti campi.

- **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.
- **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`
- **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.

- eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete
- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.ARN`, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.ARN` campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

b. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere gli eventi di dati per due bucket S3 dagli eventi di dati registrati nel tuo event data store, puoi impostare il campo su Resources.arn, impostare l'operatore for does not start con e quindi incollare un bucket S3 ARN per il quale non desideri registrare gli eventi.

   Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

   CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di

valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

c. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

16. Per aggiungere un tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati. Ripeti i passaggi 12 di questo passaggio per configurare i selettori di eventi avanzati per il tipo di risorsa.

17. Per registrare gli eventi di attività di rete, scegli Eventi di attività di rete. Gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

    Per registrare gli eventi di attività di rete, procedi come segue:

    a. Da Origine eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.

    b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.

    c. (Facoltativo) Inserisci un nome per identificare il selettore. Il nome del selettore è elencato come Nome nel selettore di eventi avanzato ed è visualizzabile se si espande la vista JSON.

    d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

        i. Per escludere o includere gli eventi di attività di rete, puoi scegliere tra i seguenti campi nella console.

            - **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi usarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
            - **`errorCode`**— È possibile utilizzarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.

- **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

18. Scegli gli eventi di Insights se desideri che il tuo percorso registri gli eventi di CloudTrail Insights.

    In Event type (Tipo di evento), seleziona Insights events (Eventi Insights). In Insights events (Eventi Insights), scegli API calls rate (Tasso di chiamata API), API error rate (Tasso di errore API), o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.

    CloudTrail Insights analizza gli eventi di gestione alla ricerca di attività insolite e registra gli eventi quando vengono rilevate anomalie. Per impostazione predefinita, i trail non registrano gli eventi Insights. Per ulteriori informazioni sugli eventi Insights, consulta Lavorare con CloudTrail Insights. Per la registrazione degli eventi Insights vengono applicati costi aggiuntivi. Per i CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

    Gli eventi Insights vengono inviati a una cartella diversa denominata `/CloudTrail-Insight` con lo stesso bucket S3, specificata nell'area Storage location della pagina dei dettagli del percorso. CloudTrailcrea il nuovo prefisso per te. Ad esempio, se il bucket S3 di destinazione corrente è denominato `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail/`, il nome del bucket S3 con un nuovo prefisso viene denominato `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail-Insight/`.

19. Al termine della scelta dei tipi di evento da registrare, scegli Next (Successivo).

20. Nella pagina Review and create (Verifica e crea), esamina le opzioni selezionate. Scegli Edit (Modifica) in una sezione per modificare le impostazioni del percorso mostrate al suo interno. Quando sei pronto per creare il percorso, scegli Create trail (Crea percorso).

21. Il nuovo trail viene visualizzato nella pagina Trails (Trail). La creazione di un percorso organizzativo può richiedere fino a 24 ore in tutte le regioni abilitate e in tutti gli account dei

membri. Nella pagina Trails (Trail) sono visualizzati i trail di tutte le regioni nell'account. In circa 5 minuti, CloudTrail pubblica file di registro che mostrano le chiamate AWS API effettuate nell'organizzazione. Puoi visualizzare i file di log nel bucket Amazon S3 specificato.

> **Note**
>
> Non è possibile rinominare un trail dopo che è stato creato. Al contrario, è possibile eliminarlo e crearne uno nuovo.

Passaggi successivi

Dopo aver creato il trail, è possibile tornare al trail per apportarvi modifiche:

- Cambiare la configurazione del trail modificandolo. Per ulteriori informazioni, consulta Aggiornamento di un percorso con la CloudTrail console.
- Se necessario, configura il bucket Amazon S3 per permettere a utenti specifici in account membri di leggere i file di log per l'organizzazione. Per ulteriori informazioni, consulta Condivisione di file di CloudTrail registro tra AWS account.
- Configura CloudTrail per inviare i file di registro a CloudWatch Logs. Per ulteriori informazioni, vedere Invio di eventi ai registri CloudWatch e la voce CloudWatch Logs in. Preparazione per la creazione di un percorso per la tua organizzazione

  > **Note**
  >
  > Solo l'account di gestione può configurare un gruppo di log CloudWatch Logs per un percorso organizzativo.

- Crea una tabella e utilizzala per eseguire una query in Amazon Athena per analizzare le attività del servizio AWS . Per ulteriori informazioni, consulta Creare una tabella per CloudTrail i log nella CloudTrail console nella Guida per l'utente di Amazon Athena.
- Aggiungere tag (coppie chiave-valore) personalizzati al trail.
- Per creare un altro trail dell'organizzazione, tornare alla pagina Trails (Trail) e scegliere Add new trail (Aggiungi nuovo trail).

> **Note**
>
> Durante la configurazione di un percorso, puoi scegliere un bucket Amazon S3 e un argomento SNS appartenenti a un altro account. Tuttavia, se desideri inviare eventi CloudTrail a un gruppo di log di CloudWatch Logs, devi scegliere un gruppo di log esistente nel tuo account corrente.

Creare un percorso per un'organizzazione con AWS CLI

Puoi creare un trail dell'organizzazione utilizzando l' AWS CLI. AWS CLI viene aggiornato regolarmente con funzionalità e comandi aggiuntivi. Per garantire il successo, assicurati di aver installato o aggiornato a una AWS CLI versione recente prima di iniziare.

> **Note**
>
> Gli esempi in questa sezione sono specifici per la creazione e l'aggiornamento di trail dell'organizzazione. Per esempi di utilizzo di AWS CLI per gestire i sentieri, vedi Gestire i percorsi con AWS CLI eConfigurazione del monitoraggio CloudWatch dei registri con AWS CLI. Quando si crea o si aggiorna un percorso organizzativo con AWS CLI, è necessario utilizzare un AWS CLI profilo nell'account di gestione o nell'account amministratore delegato con autorizzazioni sufficienti. Se stai convertendo un percorso dell'organizzazione in un percorso non dell'organizzazione, devi utilizzare l'account di gestione dell'organizzazione. Devi configurare il bucket Amazon S3 utilizzato per un percorso dell'organizzazione con autorizzazioni sufficienti.

Creazione o aggiornamento di un bucket Amazon S3 da utilizzare per archiviare i file di log per un percorso dell'organizzazione

Devi specificare un bucket Amazon S3 per ricevere i file di log per un percorso dell'organizzazione. Questo bucket deve avere una politica che CloudTrail consenta di inserire i file di registro dell'organizzazione nel bucket.

Di seguito è riportato un esempio di policy per un bucket Amazon S3 denominato*amzn-s3-demo-bucket*, di proprietà dell'account di gestione dell'organizzazione. Sostituisci *amzn-s3-demo-bucketregion*,*managementAccountID*,*trailName*, e *o-organizationID* con i valori della tua organizzazione

Questa policy del bucket contiene tre istruzioni.

- La prima istruzione consente di CloudTrail richiamare l'`GetBucketAcl`azione Amazon S3 sul bucket Amazon S3.
- La seconda istruzione consente la registrazione nel caso in cui il percorso venga modificato da percorso dell'organizzazione a percorso solo per quell'account.
- La terza istruzione consente la registrazione di un percorso dell'organizzazione.

Il criterio di esempio include una chiave di condizione `aws:SourceArn` per la policy del bucket Amazon S3. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la CloudTrail scrittura nel bucket S3 sia valida solo per uno o più percorsi specifici. In un trail dell'organizzazione, il valore di `aws:SourceArn` deve essere un ARN trail di proprietà dell'account di gestione e utilizza l'ID dell'account di gestione.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/
AWSLogs/managementAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/AWSLogs/o-
organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Questa policy di esempio non consente agli utenti degli account membri di accedere ai file di log creati per l'organizzazione. Per impostazione predefinita, i file di log dell'organizzazione sono accessibili solo per l'account di gestione. Per informazioni su come permettere l'accesso in lettura al bucket Amazon S3 per gli utenti IAM degli account membri, consulta Condivisione di file di CloudTrail registro tra AWS account.

Abilitazione CloudTrail come servizio affidabile in AWS Organizations

Prima di poter creare un percorso dell'organizzazione, devi abilitare tutte le caratteristiche in Organizations. Per ulteriori informazioni, consulta Abilitazione di tutte le caratteristiche nell'organizzazione oppure esegui il comando seguente utilizzando un profilo con autorizzazioni sufficienti nell'account di gestione:

```
aws organizations enable-all-features
```

Dopo aver abilitato tutte le funzionalità, è necessario configurare Organizations to trust CloudTrail come servizio affidabile.

Per creare una relazione di servizio affidabile tra AWS Organizations e CloudTrail, apri un terminale o una riga di comando e usa un profilo nell'account di gestione. Eseguire il comando `aws organizations enable-aws-service-access` come dimostrato nel seguente esempio.

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

Utilizzo di create-trail

Creazione di un percorso dell'organizzazione che si applica a tutte le Regioni

Per creare un percorso dell'organizzazione che si applica a tutte le Regioni, aggiungi le opzioni `--is-organization-trail` e `--is-multi-region-trail`.

> **Note**
>
> Quando si crea un percorso organizzativo con AWS CLI, è necessario utilizzare un AWS CLI profilo nell'account di gestione o nell'account amministratore delegato con autorizzazioni sufficienti.

L'esempio seguente crea un percorso dell'organizzazione che distribuisce i log da tutte le Regioni in un bucket esistente denominato *amzn-s3-demo-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
organization-trail --is-multi-region-trail
```

Per confermare che il percorso esiste in tutte le Regioni, i parametri `IsOrganizationTrail` e `IsMultiRegionTrail` nell'output sono entrambi impostati su `true`:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

> **Note**
>
> Esegui il comando `start-logging` per avviare la registrazione per il percorso. Per ulteriori informazioni, consulta Arresto e avvio della registrazione di log per un trail.

Creazione di un percorso dell'organizzazione come percorso basato su una singola Regione

Il comando seguente crea un percorso organizzativo che registra solo gli eventi in un unico percorso Regione AWS, noto anche come itinerario a regione singola. La AWS regione in cui vengono registrati gli eventi è la regione specificata nel profilo di configurazione per. AWS CLI

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
organization-trail
```

Per ulteriori informazioni, consulta Requisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS.

Output di esempio:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
```

```
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Per impostazione predefinita, il comando `create-trail` crea un percorso basato su una singola Regione che non permette la convalida dei file di log.

> **Note**
>
> Esegui il comando `start-logging` per avviare la registrazione per il percorso.

Esecuzione di update-trail per aggiornare un percorso dell'organizzazione

Puoi eseguire il comando `update-trail` per modificare le impostazioni di configurazione per un percorso dell'organizzazione o per applicare un percorso esistente per un singolo account AWS a un'intera organizzazione. Ricorda che puoi eseguire il comando `update-trail` solo dalla Regione in cui è stato creato il percorso.

> **Note**
>
> Se usi il AWS CLI o uno dei AWS SDKs per aggiornare un percorso, assicurati che la policy del bucket del percorso sia. up-to-date Per ulteriori informazioni, consulta Creare un percorso per un'organizzazione con AWS CLI.
> Quando si aggiorna un percorso organizzativo con il AWS CLI, è necessario utilizzare un AWS CLI profilo nell'account di gestione o nell'account amministratore delegato con autorizzazioni sufficienti. Se si desidera convertire un percorso dell'organizzazione in uno non dell'organizzazione, è necessario utilizzare l'account di gestione dell'organizzazione, poiché l'account di gestione è il proprietario di tutte le risorse dell'organizzazione.
> CloudTrail aggiorna gli itinerari organizzativi negli account dei membri anche se la convalida di una risorsa fallisce. Alcuni esempi di errori di convalida includono:
>
> - una policy sui bucket Amazon S3 errata
> - una politica tematica di Amazon SNS errata
> - impossibilità di effettuare consegne a un gruppo di CloudWatch log di Logs
> - autorizzazione insufficiente per crittografare utilizzando una chiave KMS

Un account membro con CloudTrail autorizzazioni può visualizzare eventuali errori di convalida di un percorso organizzativo visualizzando la pagina dei dettagli del percorso sulla CloudTrail console o eseguendo il comando. AWS CLI get-trail-status

Applicazione di un trail esistente a un'organizzazione

Per modificare un percorso esistente in modo che si applichi anche a un'organizzazione anziché a un singolo AWS account, aggiungi l'`--is-organization-trail`opzione, come mostrato nell'esempio seguente.

> **Note**
>
> Utilizza l'account di gestione per modificare un percorso non dell'organizzazione esistente in un percorso dell'organizzazione.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Per confermare che il percorso ora è valido per l'organizzazione, il parametro `IsOrganizationTrail` nell'output ha il valore `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Nell'esempio precedente, il percorso è stato configurato come percorso multiregionale ()`"IsMultiRegionTrail": true`. Un percorso che si applica a una singola Regione visualizzerebbe `"IsMultiRegionTrail": false` nell'output.

Conversione di un itinerario organizzativo a regione singola in un itinerario organizzativo multiregionale

Per convertire un organigramma a regione singola esistente in un organigramma multiregionale, aggiungi l'`--is-multi-region-trail`opzione come illustrato nell'esempio seguente.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Per confermare che l'itinerario è ora un percorso multiregionale, verificate che il `IsMultiRegionTrail` parametro nell'output abbia un valore di. `true`

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Risoluzione dei problemi relativi a un percorso organizzativo

Questa sezione fornisce informazioni su come risolvere i problemi relativi a un organigramma.

Argomenti

- CloudTrail non offre eventi
- CloudTrail non invia notifiche Amazon SNS per un account membro in un'organizzazione

CloudTrail non offre eventi

If CloudTrail non fornisce file di CloudTrail log al bucket Amazon S3

Verifica se c'è un problema con il bucket S3.

- Dalla CloudTrail console, controlla la pagina dei dettagli del percorso. Se c'è un problema con il bucket S3, la pagina dei dettagli include un avviso che indica che la consegna al bucket S3 non è riuscita.

- Da, esegui il AWS CLI comando. get-trail-status In caso di errore, l'output del comando include il `LatestDeliveryError` campo, che mostra tutti gli errori di Amazon S3 che si sono CloudTrail verificati durante il tentativo di inviare i file di log al bucket designato. Questo errore si verifica solo quando c'è un problema con il bucket S3 di destinazione e non si verifica per le richieste con timeout. Per risolvere il problema, correggi la policy del bucket in modo che CloudTrail possa scrivere nel bucket; oppure crea un nuovo bucket, quindi chiama `update-trail` per specificare il nuovo bucket. Per informazioni sulla policy del bucket dell'organizzazione, consulta Creare o aggiornare un bucket Amazon S3 da utilizzare per archiviare i file di registro per un percorso organizzativo.

> **Note**
>
> Se configuri erroneamente il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterà di reinviare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti a tariffe standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

CloudTrail Se non consegna i log a Logs CloudWatch

Verifica se c'è un problema con la configurazione della politica del ruolo CloudWatch Logs.

- Dalla CloudTrail console, controlla la pagina dei dettagli del percorso. Se c'è un problema con CloudWatch i registri, la pagina dei dettagli include un avviso che indica che il recapito CloudWatch dei registri non è riuscito.
- Da AWS CLI, esegui il comando. get-trail-status Se si verifica un errore, l'output del comando include il `LatestCloudWatchLogsDeliveryError` campo, che mostra tutti gli errori di CloudWatch log che si sono CloudTrail verificati durante il tentativo di recapitare i log a Logs. CloudWatch Per risolvere il problema, correggi la politica del CloudWatch ruolo Logs. Per informazioni sulla politica del ruolo CloudWatch Logs, vedere. Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio

Se non vedi l'attività di un account membro in un percorso organizzativo

Se non vedi l'attività di un account membro in un percorso organizzativo, controlla quanto segue:

- Controlla la regione di provenienza del percorso per vedere se si tratta di una regione che accetta l'iscrizione

  Sebbene la Regioni AWS maggior parte sia abilitata di default per la tua Account AWS, devi abilitare manualmente alcune regioni (dette anche regioni opzionali). Per informazioni su quali regioni sono abilitate per impostazione predefinita, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Gestione dell'account AWS Guida di riferimento. Per l'elenco delle regioni CloudTrail supportate, vedere. CloudTrail Regioni supportate

  Se il percorso organizzativo è multiregionale e la regione di origine è una regione con attivazione, gli account dei membri non invieranno attività al percorso organizzativo a meno che non scelgano il luogo in Regione AWS cui è stato creato il percorso multiregionale. Ad esempio, se crei un percorso multiregionale e scegli la regione Europa (Spagna) come regione di origine del percorso, solo gli account dei membri che hanno abilitato la regione Europa (Spagna) per il proprio account invieranno l'attività dell'account all'organigramma. Per risolvere il problema, abilita la regione di attivazione in ogni account membro della tua organizzazione. Per informazioni sull'attivazione di un'area geografica, consulta Abilitare o disabilitare una regione nella tua organizzazione nella Guida Gestione dell'account AWS di riferimento.

- Verifica se la politica dell'organizzazione basata sulle risorse è in conflitto con la politica dei ruoli collegati ai servizi CloudTrail

  CloudTrail utilizza il ruolo collegato al servizio denominato per supportare gli itinerari organizzativi. `AWSServiceRoleForCloudTrail` Questo ruolo collegato al servizio consente di CloudTrail eseguire azioni sulle risorse dell'organizzazione, ad esempio. `organizations:DescribeOrganization` Se la politica basata sulle risorse dell'organizzazione nega un'azione consentita nella politica relativa ai ruoli collegati ai servizi, non CloudTrail sarà in grado di eseguire l'azione anche se è consentita nella politica relativa ai ruoli collegati ai servizi. Per risolvere il problema, correggi la politica basata sulle risorse dell'organizzazione in modo che non neghi le azioni consentite nella politica relativa ai ruoli collegati ai servizi.

CloudTrail non invia notifiche Amazon SNS per un account membro in un'organizzazione

Quando un account membro con un percorso AWS Organizations organizzativo non invia notifiche Amazon SNS, potrebbe esserci un problema con la configurazione della policy tematica SNS. CloudTrail crea percorsi organizzativi negli account dei membri anche se la convalida di una risorsa

fallisce, ad esempio, l'argomento SNS dell'organization trail non include tutti gli account dei membri. IDs Se la policy dell'argomento SNS non è corretta, si verifica un errore di autorizzazione.

Per verificare se la policy degli argomenti SNS di un percorso presenta un errore di autorizzazione:

- Dalla CloudTrail console, controlla la pagina dei dettagli del percorso. Se si verifica un errore di autorizzazione, la pagina dei dettagli include un avviso `SNS authorization failed` e indica di correggere la politica dell'argomento SNS.
- Da AWS CLI, esegui il get-trail-statuscomando. Se si verifica un errore di autorizzazione, l'output del comando include il `LastNotificationError` campo con un valore di`AuthorizationError`. Per risolvere il problema, correggi la policy tematica di Amazon SNS. Per informazioni sulla policy tematica di Amazon SNS, consulta. Policy tematica di Amazon SNS per CloudTrail

Per ulteriori informazioni sugli argomenti relativi a SNS e sulla sottoscrizione ad essi, consulta Getting started with Amazon SNS nella Amazon Simple Notification Service Developer Guide.

Comprendere i percorsi multiregionali e le regioni opt-in

Un percorso può essere applicato a tutto ciò Regioni AWS che è abilitato nella tua Account AWS o può essere applicato a una singola regione. Un percorso che si applica a tutto Regioni AWS ciò che è abilitato nella tua Account AWS viene definito percorso multiregionale. Come best practice, consigliamo di creare un percorso multiregionale perché registra l'attività in tutte le regioni abilitate. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multiregionali. È possibile creare un percorso a regione singola solo utilizzando l'operazione AWS CLI o `CreateTrail`API.

Sebbene la Regioni AWS maggior parte sia abilitata di default per le tue Account AWS, devi abilitare manualmente alcune regioni (chiamate anche regioni opt-in). Per informazioni su quali regioni sono abilitate per impostazione predefinita, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Gestione dell'account AWS Guida di riferimento. Per l'elenco delle regioni CloudTrail supportate, vedere. CloudTrail Regioni supportate

Argomenti

- Quali sono i vantaggi dei percorsi multiregionali?
- Cosa succede quando si crea un percorso multiregionale?
- Cosa succede quando abiliti una regione opt-in?
- Cosa succede quando si disabilita una regione con consenso esplicito?

Quali sono i vantaggi dei percorsi multiregionali?

Un percorso multiregionale presenta i seguenti vantaggi:

- Le impostazioni di configurazione per il percorso si applicano in modo coerente a tutti gli utenti abilitati Regioni AWS.
- Ricevi CloudTrail eventi da tutti gli utenti abilitati Regioni AWS in un singolo bucket Amazon S3 e, facoltativamente, in un CloudWatch gruppo di log Logs.
- Puoi gestire le configurazioni dei trail per tutti i dispositivi abilitati da un'unica posizione. Regioni AWS

Cosa succede quando si crea un percorso multiregionale?

La creazione di un percorso multiregionale ha i seguenti effetti:

- CloudTrail invia i file di log per l'attività dell'account da tutti gli account abilitati Regioni AWS al singolo bucket Amazon S3 specificato e, facoltativamente, a un CloudWatch gruppo di log Logs.
- Se hai configurato un argomento Amazon SNS per il percorso, le notifiche SNS sulle consegne di file di log in all enabled Regioni AWS vengono inviate a quel singolo argomento SNS.
- Puoi vedere il percorso multiregionale in tutte le versioni abilitate Regioni AWS, ma puoi modificare solo il percorso nella regione di origine in cui è stato creato.

Cosa succede quando abiliti una regione opt-in?

Dopo aver abilitato una regione opt-in, CloudTrail crea una copia identica di ogni percorso multiregionale nella regione opt-in che hai abilitato.

CloudTrail utilizza un modello di calcolo distribuito chiamato eventuale consistenza. Poiché l'attivazione di una regione richiede da alcuni minuti a diverse ore, è possibile che non vengano visualizzati immediatamente tutti gli eventi nei registri della regione appena abilitata. La consegna di tutti i log CloudTrail per la nuova regione abilitata potrebbe richiedere fino a diverse ore. Durante questo periodo, è possibile visualizzare gli ultimi 90 giorni di eventi di gestione registrati in quella regione visualizzando la cronologia CloudTrail degli eventi o eseguendo il aws cloudtrail lookup-events --region <region>comando. La cronologia degli eventi è attiva per impostazione predefinita in una regione Account AWS, registra gli ultimi 90 giorni di eventi di gestione registrati in una regione e non richiede una traccia.

Per informazioni sull'attivazione di una regione opzionale per la tua Account AWS, consulta Abilitare o disabilitare una regione per gli account autonomi o Abilitare o disabilitare una regione nell'organizzazione.

Cosa succede quando si disabilita una regione con consenso esplicito?

Poiché il tuo account potrebbe avere attività nella regione che hai disabilitato, ad esempio azioni Servizi AWS per rimuovere risorse, continuerà a registrare attività e CloudTrail tenterà di inviare eventi al bucket S3 per tutti i percorsi che non vengono eliminati prima della disattivazione della regione.

Copiare gli eventi del percorso su CloudTrail Lake

È possibile copiare gli eventi del percorso esistenti in un archivio dati di eventi CloudTrail Lake per creare un' point-in-timeistantanea degli eventi registrati nel percorso. La copia degli eventi traccia non interferisce con la capacità della traccia di registrare gli eventi e non modifica in alcun modo la traccia.

Puoi copiare gli eventi del trail in un data store di eventi esistente configurato per CloudTrail gli eventi oppure puoi creare un nuovo CloudTrail event data store e scegliere l'opzione Copia gli eventi del trail come parte della creazione del data store degli eventi. Per ulteriori informazioni sulla copia degli eventi di percorso in un datastore di eventi esistente, consulta Copia gli eventi del trail in un data store di eventi esistente utilizzando la console CloudTrail . Per ulteriori informazioni sulla creazione di un nuovo datastore di eventi, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

La copia degli eventi del trail in un data store di eventi CloudTrail Lake consente di eseguire query sugli eventi copiati. CloudTrail Le query Lake offrono una visione più approfondita e personalizzabile degli eventi rispetto alle semplici ricerche di chiavi e valori nella cronologia degli eventi o in esecuzione. `LookupEvents` Per ulteriori informazioni su CloudTrail Lake, vedere. Lavorare con AWS CloudTrail Lake

Se stai copiando gli eventi del trail in un datastore di eventi dell'organizzazione, dovrai utilizzare l'account di gestione dell'organizzazione. Non puoi copiare gli eventi del trail utilizzando l'account dell'amministratore delegato di un'organizzazione.

CloudTrail I Lake Event Data Store sono a pagamento. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello

massimo per il datastore di eventi. Per informazioni sui CloudTrail prezzi e sulla gestione dei costi di Lake, vedi AWS CloudTrail Prezzi e. Gestione dei costi CloudTrail del lago

Quando copi gli eventi del trail in un CloudTrail Lake Event Data Store, ti vengono addebitati dei costi in base alla quantità di dati non compressi che l'Event Data Store acquisisce.

Quando copi gli eventi del trail su CloudTrail Lake, CloudTrail decomprime i log archiviati in formato gzip (compresso) e quindi copia gli eventi contenuti nei log nel tuo archivio dati degli eventi. La dimensione dei dati non compressi potrebbe essere maggiore della dimensione di archiviazione effettiva di S3. Per avere una stima generale della dimensione dei dati non compressi, puoi moltiplicare la dimensione dei log nel bucket S3 per 10.

È possibile ridurre i costi specificando un intervallo di tempo più ristretto per gli eventi copiati. Se intendi utilizzare il datastore di eventi solo per le query sugli eventi copiati, puoi disattivare l'importazione degli eventi ed evitare così di incorrere in addebiti per eventi futuri. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail e Gestione dei costi CloudTrail del lago.

Scenari

La tabella seguente descrive alcuni scenari comuni per la copia degli eventi di percorso e come realizzare ogni scenario utilizzando la console.

Scenario	Come posso eseguire questa operazione nella console?
Analizza e interroga gli eventi storici del trail in Lake senza importare nuovi eventi CloudTrail	Crea un nuovo datastore di eventi e scegli l'opzione Copia gli eventi del percorso come parte della creazione del datastore di eventi. Durante la creazione del datastore di eventi, deselezio na Eventi di importazione (passaggio 15 della procedura) per assicurarti che il datastore di eventi contenga solo gli eventi storici del percorso e nessun evento futuro.
Sostituisci il percorso esistente con un archivio dati CloudTrail sugli eventi Lake	Crea un datastore di eventi con gli stessi selettori di eventi del tuo percorso per assicurarti che il datastore di eventi abbia la stessa copertura del tuo percorso. Per evitare la duplicazione degli eventi tra il percorso di origine e il datastore di eventi di destinazione, scegli un intervallo di date per gli eventi copiati che sia precedente alla creazione del datastore di eventi.

Scenario	Come posso eseguire questa operazione nella console?
	Dopo la creazione del datastore di eventi, potrai disattivare la registrazione per il percorso ed evitare così costi aggiuntivi.

Argomenti

- Considerazioni sulla copia di eventi di percorso
- Autorizzazioni necessarie per la copia di eventi traccia
- Copia gli eventi del trail in un data store di eventi esistente utilizzando la console CloudTrail

Considerazioni sulla copia di eventi di percorso

Quando copi eventi traccia, considera i fattori seguenti.

- Quando copi gli eventi del trail, CloudTrail utilizza l'operazione `GetObject`API S3 per recuperare gli eventi del trail nel bucket S3 di origine. Esistono alcune classi di archiviazione archiviata di S3, come i livelli recupero flessibile S3 Glacier, Deep Archive S3 Glacier, S3 Outposts e Deep Archive Piano intelligente Amazon S3 che non sono accessibili tramite l'utilizzo di `GetObject`. Per copiare gli eventi di percorso archiviati in queste classi di archiviazione archiviate, devi prima ripristinare una copia utilizzando l'operazione S3 `RestoreObject`. Per informazioni sul ripristino di oggetti archiviati, consulta Ripristino di oggetti archiviati nella Guida per l'utente di Amazon S3.
- Quando copi gli eventi di trail in un event data store, CloudTrail copia tutti gli eventi di trail indipendentemente dalla configurazione dei tipi di eventi dell'Event Data Store di destinazione, dai selettori di eventi avanzati o. Regione AWS
- Prima di copiare gli eventi del percorso in un datastore di eventi esistente, assicurati che l'opzione di prezzo e il periodo di conservazione del datastore di eventi siano configurati correttamente per il tuo caso d'uso.
  - Opzione di prezzo: l'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi. Per ulteriori informazioni su opzioni di prezzo, consulta Prezzi AWS CloudTrail e Opzioni di prezzo del datastore di eventi.
  - Periodo di conservazione: il periodo di conservazione determina per quanto tempo i dati degli eventi vengono conservati nell'archivio dati degli eventi. CloudTrail copia solo gli eventi trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'Event Data Store

(periodo di conservazione = `oldest-event-in-days` +`number-days-to-retain`). Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.

- Se stai copiando gli eventi di percorso in un datastore di eventi per analizzarli e non desideri importare eventi futuri, puoi interrompere l'importazione nel datastore. Durante la creazione del datastore di eventi, deseleziona l'opzione Eventi di importazione (passaggio 15 della procedura) per assicurarti che il datastore di eventi contenga solo gli eventi storici del percorso e nessun evento futuro.
- Prima di copiare gli eventi trail, disabilita tutte le liste di controllo degli accessi (ACLs) allegate al bucket S3 di origine e aggiorna la policy del bucket S3 per il data store degli eventi di destinazione. Per ulteriori informazioni sull'aggiornamento della policy del bucket S3, consulta Policy del bucket Amazon S3 per la copia di eventi traccia. Per ulteriori informazioni sulla disabilitazione ACLs, consulta Controllo della proprietà degli oggetti e disabilitazione del bucket. ACLs
- CloudTrail copia solo gli eventi trail dai file di registro compressi con Gzip che si trovano nel bucket S3 di origine. CloudTrail non copia gli eventi di trail da file di registro non compressi o file di registro compressi utilizzando un formato diverso da Gzip.
- Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, per gli eventi copiati scegli un intervallo di tempo precedente alla creazione dell'archivio dati degli eventi.
- Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel prefisso del bucket S3 e i `CloudTrail` prefissi all'interno del prefisso e non controlla i prefissi per `CloudTrail` altri servizi. AWS Se desideri copiare CloudTrail gli eventi contenuti in un altro prefisso, devi scegliere il prefisso quando copi gli eventi trail.
- Per copiare gli eventi del trail in un datastore di eventi dell'organizzazione, devi utilizzare l'account di gestione dell'organizzazione. Non puoi utilizzare l'account dell'amministratore delegato per copiare gli eventi di trail in un archivio dati di eventi di un'organizzazione.

Autorizzazioni necessarie per la copia di eventi traccia

Prima di copiare gli eventi trail, assicurati di disporre di tutte le autorizzazioni necessarie per il tuo ruolo IAM. Devi aggiornare le autorizzazioni del ruolo IAM solo se scegli un ruolo IAM esistente per la copia di eventi traccia. Se scegli di creare un nuovo ruolo IAM, CloudTrail fornisce tutte le autorizzazioni necessarie per il ruolo.

Se il bucket S3 di origine utilizza una chiave KMS per la crittografia dei dati, assicurati che la policy della chiave KMS CloudTrail consenta di decrittografare i dati nel bucket. Se il bucket S3 di origine

utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail

Argomenti

- Autorizzazioni IAM per la copia di eventi traccia
- Policy del bucket Amazon S3 per la copia di eventi traccia
- Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine

Autorizzazioni IAM per la copia di eventi traccia

Quando copi eventi traccia, puoi creare un nuovo ruolo IAM o utilizzare un ruolo IAM esistente. Quando scegli un nuovo ruolo IAM, CloudTrail crea un ruolo IAM con le autorizzazioni richieste e non sono necessarie ulteriori azioni da parte tua.

Se scegli un ruolo esistente, assicurati che le policy del ruolo IAM consentano di copiare CloudTrail gli eventi del trail dal bucket S3 di origine. Questa sezione fornisce esempi delle policy di attendibilità e di autorizzazione necessarie al ruolo IAM.

L'esempio seguente fornisce la politica di autorizzazione, che consente di copiare gli eventi CloudTrail di trail dal bucket S3 di origine. Sostituisci*amzn-s3-demo-bucket*,*myAccountID*, *regionprefix*, e *eventDataStoreId* con i valori appropriati per la tua configurazione. *myAccountID*È l'ID dell' AWS account utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

Sostituisci *key-region* e *keyID* con i valori della chiave KMS utilizzata per crittografare il bucket S3 di origine. *keyAccountID* Se il bucket S3 di origine non utilizza una chiave KMS per la crittografia, puoi omettere l'istruzione `AWSCloudTrailImportKeyAccess`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

L'esempio seguente fornisce la policy di fiducia IAM, che consente di assumere un ruolo IAM CloudTrail per copiare gli eventi del trail dal bucket S3 di origine. Sostituisci *myAccountID* e *eventDataStoreArn* con i valori appropriati per la tua configurazione. *region* *myAccountID*È l' Account AWS ID utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

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

```
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Policy del bucket Amazon S3 per la copia di eventi traccia

Per impostazione predefinita, i bucket e gli oggetti Amazon S3 sono privati. Solo il proprietario della risorsa (l'account AWS che ha creato il bucket) può accedere al bucket e agli oggetti in esso contenuti. Il proprietario della risorsa può concedere le autorizzazioni di accesso ad altre risorse e ad altri utenti mediante una policy di accesso.

Prima di copiare gli eventi di trail, devi aggiornare la policy del bucket S3 per consentire CloudTrail di copiare gli eventi di trail dal bucket S3 di origine.

Puoi aggiungere la seguente dichiarazione alla policy del bucket S3 per concedere queste autorizzazioni. Sostituisci *roleArn* e *amzn-s3-demo-bucket* con i valori appropriati per la tua configurazione.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
```

```
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine

Se il bucket S3 di origine utilizza una chiave KMS per la crittografia dei dati, assicurati che la policy delle chiavi KMS fornisca le `kms:GenerateDataKey` autorizzazioni necessarie per copiare gli eventi del trail da un bucket S3 CloudTrail con la `kms:Decrypt` crittografia SSE-KMS abilitata. Se il bucket S3 di origine utilizza più chiavi KMS, è necessario aggiornare la policy di ogni chiave. L'aggiornamento della policy delle chiavi KMS consente di decrittografare i dati nel bucket S3 di origine, eseguire controlli di convalida CloudTrail per garantire che gli eventi siano conformi agli standard e copiare gli eventi nel Lake Event Data Store. CloudTrail CloudTrail

L'esempio seguente fornisce la politica delle chiavi KMS, che consente di CloudTrail decrittografare i dati nel bucket S3 di origine. Sostituisci*roleArn*,*amzn-s3-demo-bucket*, *myAccountIDregion*, e *eventDataStoreId* con i valori appropriati per la tua configurazione. *myAccountID*È l'ID dell' AWS account utilizzato per CloudTrail Lake, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
```

```
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

Copia gli eventi del trail in un data store di eventi esistente utilizzando la console CloudTrail

Utilizza la procedura seguente per copiare eventi di percorso in un datastore di eventi esistente. Per ulteriori informazioni su come creare un nuovo datastore di eventi, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

> **Note**
>
> Prima di copiare gli eventi del percorso in un datastore di eventi esistente, assicurati che l'opzione di prezzo e il periodo di conservazione del datastore di eventi siano configurati correttamente per il tuo caso d'uso.
>
> - Opzione di prezzo: l'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi. Per ulteriori informazioni su opzioni di prezzo, consulta Prezzi AWS CloudTrail e Opzioni di prezzo del datastore di eventi.
> - Periodo di conservazione: il periodo di conservazione determina per quanto tempo i dati degli eventi vengono conservati nell'archivio dati degli eventi. CloudTrail copia solo gli eventi trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Per determinare il periodo di conservazione appropriato, prendi la somma dell'evento più vecchio che desideri copiare in giorni e il numero di giorni in cui desideri conservare gli eventi nell'Event Data Store (periodo di conservazione = *oldest-event-in-days* +*number-days-to-retain*). Ad esempio, se l'evento più vecchio da copiare risale a 45 giorni fa e desideri conservare gli eventi nel datastore di eventi per altri 45 giorni, imposta il periodo di conservazione su 90 giorni.

Per copiare eventi del percorso in un datastore di eventi

1. Accedi AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.

2. Scegli Trails nel riquadro di navigazione a sinistra della CloudTrail console.
3. Nella pagina Trails (Percorsi), scegliere il percorso, quindi Copy events to Lake (Copia eventi in Lake). Se il bucket S3 di origine per il trail utilizza una chiave KMS per la crittografia dei dati, assicurati che la policy della chiave KMS CloudTrail consenta di decrittografare i dati nel bucket. Se il bucket S3 di origine utilizza più chiavi KMS, devi aggiornare la policy di ciascuna chiave per consentire la decrittografia dei dati nel bucket. CloudTrail Per ulteriori informazioni sull'aggiornamento della policy delle chiavi KMS, consulta Policy delle chiavi KMS per la decrittografia dei dati nel bucket S3 di origine.
4. (Facoltativo) Per impostazione predefinita, copia CloudTrail solo CloudTrail gli eventi contenuti nel prefisso del bucket S3 e i prefissi all'interno del `CloudTrail` prefisso e non controlla i prefissi per altri servizi. `CloudTrail` AWS Se desideri copiare gli CloudTrail eventi contenuti in un altro prefisso, scegli Inserisci URI S3, quindi scegli Browse S3 per cercare il prefisso.

   La policy del bucket S3 deve concedere CloudTrail l'accesso ai copy trail events. Per ulteriori informazioni sull'aggiornamento della policy del bucket S3, consulta Policy del bucket Amazon S3 per la copia di eventi traccia.
5. Per Specificare un intervallo di tempo di eventi, scegli l'intervallo di tempo per copiare gli eventi. CloudTrail controlla il prefisso e il nome del file di registro per verificare che il nome contenga una data compresa tra la data di inizio e di fine scelte prima di tentare di copiare gli eventi del trail. Puoi scegliere un Intervallo relativo o un Intervallo assoluto. Per evitare la duplicazione degli eventi tra l'archivio dati degli eventi traccia di origine e quello di destinazione, scegliere un intervallo di tempo antecedente alla creazione dell'archivio dati degli eventi.

   > **Note**
   >
   > CloudTrail copia solo gli eventi di trail che `eventTime` rientrano nel periodo di conservazione dell'Event Data Store. Ad esempio, se il periodo di conservazione di un Event Data Store è di 90 giorni, non CloudTrail copierà alcun evento di trail con una data `eventTime` più vecchia di 90 giorni.

   - Se scegli Intervallo relativo, puoi scegliere di copiare gli eventi registrati negli ultimi 6 mesi, 1 anno, 2 anni, 7 anni o un intervallo personalizzato. CloudTrail copia gli eventi registrati nel periodo di tempo scelto.
   - Se scegli l'intervallo assoluto, puoi scegliere una data di inizio e di fine specifica. CloudTrail copia gli eventi che si sono verificati tra le date di inizio e di fine scelte.

6. Per Luogo di distribuzione, scegli l'archivio dati degli eventi di destinazione dall'elenco a discesa.
7. Per Autorizzazioni, scegli una delle opzioni seguenti del ruolo IAM. Se scegli un ruolo IAM esistente, accertati che la policy dei ruoli IAM fornisca le autorizzazioni necessarie. Per ulteriori informazioni sull'aggiornamento delle autorizzazioni del ruolo IAM, consultare Autorizzazioni IAM per la copia di eventi traccia
   - Scegli Creare un nuovo ruolo (consigliato) per creare un nuovo ruolo IAM. Per Inserisci il nome del ruolo IAM, inserisci un nome per il ruolo. CloudTrail crea automaticamente le autorizzazioni necessarie per questo nuovo ruolo.
   - Scegli Usa un ruolo IAM personalizzato ARN per utilizzare un ruolo IAM personalizzato non elencato. Per Inserisci ARN ruolo IAM, inserisci l'ARN IAM.
   - Scegli un ruolo IAM esistente dall'elenco a discesa.
8. Scegli Copia eventi.
9. Viene chiesto di confermare la copia. Quando sei pronto a confermare, scegli Copia eventi traccia in Lake, quindi Copia eventi.
10. Nella pagina Dettagli copia, puoi visualizzare lo stato della copia ed esaminare eventuali errori. Quando la copia di un evento traccia viene completata, il relativo Stato copia viene impostato su Completato in assenza di errori o su Non riuscito se si sono verificati errori.

    > **Note**
    >
    > I dettagli mostrati nella pagina dei dettagli della copia dell'evento non sono in tempo reale. I valori effettivi per dettagli come i prefissi copiati potrebbero essere superiori a quelli mostrati nella pagina. CloudTrail aggiorna i dettagli in modo incrementale nel corso della copia dell'evento.

11. Se Stato copia è Non riuscito, correggi eventuali errori mostrati in Errori di copia e scegli Riprova la copia. Quando si riprova una copia, la CloudTrail riprende nella posizione in cui si è verificato l'errore.

Per ulteriori informazioni sulla visualizzazione dei dettagli di una copia evento traccia, consulta Visualizza i dettagli della copia dell'evento con la console CloudTrail .

Acquisizione e visualizzazione dei file di CloudTrail registro

Dopo aver creato un trail e averlo configurato per acquisire i file di log desiderati, devi essere in grado di individuare i file di log e interpretare le informazioni in essi contenute.

CloudTrail consegna i tuoi file di log a un bucket Amazon S3 specificato al momento della creazione del trail. CloudTrail in genere consegna i log entro una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail. Gli eventi di Insights in genere vengono distribuiti nel bucket entro 30 minuti dall'attività insolita. Dopo aver abilitato gli eventi Insights per la prima volta, attendi fino a 36 ore per visualizzare i primi eventi Insights se viene rilevata un'attività insolita.

> **Note**
>
> Se configuri male il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterai di recapitare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti ai costi standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Argomenti

- Trovare i file di registro CloudTrail
- Scaricamento dei file di CloudTrail registro

Trovare i file di registro CloudTrail

CloudTrail pubblica i file di registro nel tuo bucket S3 in un archivio gzip. Nel bucket S3, il file di log ha un nome formattato che include i seguenti elementi:

- Il nome del bucket che hai specificato quando hai creato il trail (disponibile nella pagina Trails della console) CloudTrail
- Prefisso (opzionale) specificato durante la creazione del trail
- La stringa "» AWSLogs
- Numero di account
- La stringa "CloudTrail»

- Un identificatore della regione, ad esempio us-west-1
- Anno di pubblicazione del file di log nel formato YYYY
- Mese di pubblicazione del file di log nel formato MM
- Giorno di pubblicazione del file di log nel formato DD
- Stringa alfanumerica che disambigua il file dagli altri inclusi nello stesso periodo di tempo

L'esempio seguente mostra un nome di oggetto file di log completo:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> Per gli itinerari organizzativi, il nome dell'oggetto del file di registro nel bucket S3 include l'ID dell'unità organizzativa nel percorso, come segue:
>
> ```
> amzn-s3-demo-bucket/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

Per recuperare un file di log, puoi utilizzare la console Amazon S3, l'interfaccia a riga di comando (CLI) o l'API Amazon S3.

Per trovare i file di log mediante la console Amazon S3

1. Apri la console Amazon S3.
2. Scegliere il bucket specificato.
3. Esplorare la gerarchia di oggetti fino a trovare il file di log desiderato.

   Tutti i file di log hanno l'estensione .gz.

Potrai navigare in una gerarchia di oggetti simile a quella dell'esempio seguente, ma con valori diversi per nome di bucket, ID account, Regione e data.

```
All Buckets
```

```
    amzn-s3-demo-bucket
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

Un file di log per la precedente gerarchia di oggetti sarà simile alla seguente:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> Anche se è una possibilità non comune, è possibile ricevere file di log contenenti uno o più eventi duplicati. Nella maggior parte dei casi, gli eventi duplicati avranno lo stesso `eventID`. Per ulteriori informazioni sul campo `eventID`, consulta CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

Scaricamento dei file di CloudTrail registro

I file di log sono in formato JSON. Se disponi di un visualizzatore JSON aggiuntivo installato, puoi visualizzare i file direttamente nel tuo browser. Devi fare doppio clic sul nome del file di log nel bucket per aprire una nuova finestra o scheda del browser. Il formato JSON viene visualizzato in un formato leggibile.

CloudTrail i file di registro sono oggetti Amazon S3. Puoi utilizzare la console Amazon S3, la (AWS Command Line Interface CLI) o l'API Amazon S3 per recuperare i file di registro.

Per ulteriori informazioni, consulta la panoramica degli oggetti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

La procedura seguente descrive come scaricare un file di log con la AWS Management Console.

Per scaricare e leggere un file di log

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/

2. Scegliere il bucket e il file di log da scaricare.
3. Scegliere Download (Scarica) o Download as (Scarica come) e seguire le istruzioni per salvare il file. Questa operazione salva il file in formato compresso.

> **Note**
>
> Alcuni browser, ad esempio Chrome, estrae automaticamente il file di log. Se il browser esegue automaticamente questa operazione, passare al punto 5.

4. Usare un prodotto, ad esempio 7-Zip, per estrarre i file di log.
5. Aprire il file di log in un editor di testo, ad esempio Notepad++.

Per ulteriori informazioni sui campi di evento che possono essere visualizzati in una voce del file di log, consulta CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

AWS collabora con specialisti di terze parti in materia di registrazione e analisi per fornire soluzioni che utilizzano l' CloudTrail output. Per ulteriori informazioni, consulta AWS CloudTrail partner.

> **Note**
>
> Puoi anche utilizzare la caratteristica Event history (Cronologia eventi) per cercare gli eventi per creare, aggiornare ed eliminare le attività delle API negli ultimi 90 giorni.
> Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Configurazione delle notifiche Amazon SNS per CloudTrail

Puoi ricevere una notifica quando vengono CloudTrail pubblicati nuovi file di log nel tuo bucket Amazon S3. Le notifiche vengono gestite tramite Amazon Simple Notification Service (Amazon SNS).

Le notifiche sono opzionali. Se desideri ricevere notifiche, configuri l'invio CloudTrail di informazioni di aggiornamento a un argomento di Amazon SNS ogni volta che viene inviato un nuovo file di registro. Per ricevere queste notifiche, puoi utilizzare Amazon SNS per effettuare la sottoscrizione all'argomento desiderato. Un sottoscrittore può ricevere gli aggiornamenti inviati a una coda Amazon Simple Queue Service (Amazon SQS). Ciò consente di gestire le notifiche a livello di programmazione.

Argomenti

- Configurazione CloudTrail per l'invio di notifiche

Configurazione CloudTrail per l'invio di notifiche

Sulla CloudTrail console, puoi configurare un percorso per utilizzare un argomento Amazon SNS abilitando l'opzione di invio delle notifiche SNS quando crei o aggiorni un percorso. Se scegli di utilizzare un nuovo argomento, CloudTrail crea l'argomento Amazon SNS per te e allega una policy appropriata, in modo che CloudTrail disponga dell'autorizzazione alla pubblicazione su quell'argomento.

Con AWS CLI, puoi creare o aggiornare un percorso per utilizzare un argomento di Amazon SNS specificando un valore per il parametro. `--sns-topic-name` Puoi specificare il nome o l'ARN per l'argomento Amazon SNS.

Quando crei un nome per l'argomento SNS, il nome deve soddisfare i seguenti requisiti:

- Deve contenere da 1 a 256 caratteri.
- Deve contenere caratteri ASCII maiuscoli e minuscoli, numeri, trattini e caratteri di sottolineatura.

Quando configuri le notifiche per un percorso multiregionale, le notifiche da tutte le regioni vengono inviate all'argomento Amazon SNS specificato. In presenza di uno o più percorsi specifici di una determinata Regione, puoi creare un argomento distinto per ogni Regione ed eseguire la sottoscrizione a ciascuna di esse singolarmente.

Per ricevere notifiche, iscriviti all'argomento o agli argomenti di Amazon SNS che CloudTrail utilizza. A tale scopo puoi usare la console Amazon SNS o i comandi della CLI di Amazon SNS. Per ulteriori informazioni, consulta Sottoscrizione a un argomento di Amazon SNS nella Guida per lo Sviluppatore di Amazon Simple Notification Service.

> **Note**
>
> CloudTrail invia una notifica quando i file di log vengono scritti nel bucket Amazon S3. Un account attivo può generare un numero elevato di notifiche. Se effettui la sottoscrizione tramite e-mail o SMS, puoi ricevere un numero elevato di messaggi. Consigliamo di effettuare la sottoscrizione utilizzando Amazon Simple Queue Service (Amazon SQS), che consente di gestire le notifiche a livello di programmazione. Per ulteriori informazioni, consulta

Sottoscrizione di una coda Amazon SQS a un argomento Amazon SNS (console) nella Guida per sviluppatori di Amazon Simple Queue Service.

La notifica Amazon SNS è composta da un oggetto JSON che include un campo `Message`. Nel campo `Message` è riportato il percorso completo del file di log, come illustrato nell'esempio seguente:

```
{
    "s3Bucket": "amzn-s3-demo-bucket","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Se nel tuo bucket Amazon S3 vengono distribuiti più file di log, una notifica può contenere più log, come illustrato nell'esempio seguente:

```
{
    "s3Bucket": "amzn-s3-demo-bucket",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

Se scegli di ricevere le notifiche via e-mail, il corpo dell'e-mail include il contenuto del campo `Message`. Per informazioni sulla struttura JSON, consulta Fanout to Amazon SQS queues nella Amazon Simple Notification Service Developer Guide. Solo il campo mostra informazioni. `Message` CloudTrail Gli altri campi contengono informazioni provenienti dal servizio Amazon SNS.

Se crei un trail con l' CloudTrail API, puoi specificare un argomento Amazon SNS esistente a cui desideri CloudTrail inviare notifiche con le operazioni `CreateTrail`or `UpdateTrail`. Devi assicurarti che l'argomento esista e che disponga delle autorizzazioni che consentano di CloudTrail inviargli notifiche. Per informazioni, consulta Policy tematica di Amazon SNS per CloudTrail.

Risorse aggiuntive

Per informazioni sugli argomenti Amazon SNS e sulla relativa sottoscrizione, consulta la Guida per gli sviluppatori di Amazon Simple Notification Service.

Utilizzo AWS CloudTrail con gli endpoint VPC dell'interfaccia

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire una connessione privata tra il tuo VPC e. AWS CloudTrailÈ possibile utilizzare questa connessione per abilitare CloudTrail per comunicare con le risorse nel VPC senza accedere all'Internet pubblico.

Amazon VPC è un AWS servizio che puoi utilizzare per avviare AWS risorse in una rete virtuale definita dall'utente. Con un VPC;, detieni il controllo delle impostazioni della rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Con gli endpoint VPC, il routing tra il VPC e i AWS servizi viene gestito dalla AWS rete e puoi utilizzare le policy IAM per controllare l'accesso alle risorse del servizio.

Per connettere il tuo VPC CloudTrail, definisci un'interfaccia VPC endpoint per. CloudTrail Un endpoint di interfaccia è un'interfaccia di rete elastica con un indirizzo IP privato che funge da punto di ingresso per il traffico destinato a un servizio supportato AWS . L'endpoint fornisce una connettività affidabile e scalabile CloudTrail senza richiedere un gateway Internet, un'istanza NAT (Network Address Translation) o una connessione VPN. Per ulteriori informazioni, consulta Che cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.

Gli endpoint VPC di interfaccia sono alimentati da AWS PrivateLink, una AWS tecnologia che consente la comunicazione privata tra AWS i servizi utilizzando un'interfaccia di rete elastica con indirizzi IP privati. Per ulteriori informazioni, consulta AWS PrivateLink.

Le seguenti sezioni sono destinate agli utenti di Amazon VPC. Per ulteriori informazioni, consulta le Nozioni di base su Amazon VPC nella Guida per l'utente di Amazon VPC.

Argomenti

- Regioni
- Crea un endpoint VPC per CloudTrail
- Crea una policy per gli endpoint VPC per CloudTrail
- Sottoreti condivise

Regioni

AWS CloudTrail supporta gli endpoint VPC e le policy degli endpoint VPC in tutti i casi in cui è supportato. Regioni AWS CloudTrail

Crea un endpoint VPC per CloudTrail

Per iniziare a utilizzarlo CloudTrail con il tuo VPC, crea un endpoint VPC di interfaccia per. CloudTrail Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS con interfaccia nella Amazon VPC User Guide.

Non è necessario modificare le impostazioni per. CloudTrail CloudTrail chiama altri dispositivi Servizi AWS utilizzando endpoint pubblici o endpoint VPC con interfaccia privata, a seconda di quale dei due siano in uso.

Crea una policy per gli endpoint VPC per CloudTrail

Una policy per gli endpoint VPC è una risorsa IAM che puoi collegare a un endpoint VPC di interfaccia. La policy endpoint predefinita offre l'accesso completo all'endpoint VPC CloudTrail APIs tramite l'interfaccia. Per controllare l'accesso concesso CloudTrail dal tuo VPC, collega una policy endpoint personalizzata all'endpoint VPC di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni sulle policy degli endpoint VPC, incluso come aggiornare una policy, consulta Controlling access to services with VPC endpoint nella Amazon VPC User Guide.

Di seguito sono riportati alcuni esempi di policy endpoint VPC personalizzate per. CloudTrail

Politiche di esempio:

- Esempio: consenti tutte le CloudTrail azioni
- Esempio: consentire azioni specifiche CloudTrail
- Esempio: nega tutte le azioni CloudTrail
- Esempio: nega azioni specifiche CloudTrail

- Esempio: consenti tutte CloudTrail le azioni da un VPC specifico
- Esempio: consenti tutte CloudTrail le azioni da un endpoint VPC specifico

Esempio: consenti tutte le CloudTrail azioni

L'esempio seguente di politica degli endpoint VPC concede l'accesso a tutte le CloudTrail azioni per tutti i principali su tutte le risorse.

JSON

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

Esempio: consentire azioni specifiche CloudTrail

L'esempio seguente di politica degli endpoint VPC concede l'accesso per eseguire `cloudtrail:ListEventDataStores` le azioni `cloudtrail:ListTrails` e per tutti i principali su tutte le risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:ListTrails",
 "cloudtrail:ListEventDataStores"],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "*"
```

```
        }
    ]
}
```

Esempio: nega tutte le azioni CloudTrail

L'esempio seguente di politica degli endpoint VPC nega l'accesso a tutte le CloudTrail azioni per tutti i principali su tutte le risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "cloudtrail:*",
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Esempio: nega azioni specifiche CloudTrail

Il seguente esempio di politica degli endpoint VPC nega le `cloudtrail:CreateEventDataStore` azioni `cloudtrail:CreateTrail` e per tutti i principali su tutte le risorse.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:CreateTrail",
 "cloudtrail:CreateEventDataStore"],
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
```

```
        }
    ]
}
```

Esempio: consenti tutte CloudTrail le azioni da un VPC specifico

L'esempio seguente di politica degli endpoint VPC concede l'accesso per eseguire tutte le CloudTrail azioni per tutti i principali su tutte le risorse, ma solo se il richiedente utilizza il VPC specificato per effettuare la richiesta. *vpc-id*Sostituiscilo con il tuo ID VPC.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals": {
        "aws:SourceVpc": "vpc-1234567890abcdef0"
        }
      }
    }
  ]
}
```

Esempio: consenti tutte CloudTrail le azioni da un endpoint VPC specifico

L'esempio seguente di politica degli endpoint VPC concede l'accesso per eseguire tutte le CloudTrail azioni per tutti i principali su tutte le risorse, ma solo se il richiedente utilizza l'endpoint VPC specificato per effettuare la richiesta. *vpc-endpoint-id*Sostituiscilo con il tuo ID endpoint VPC.

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "cloudtrail:*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
        }
      }
  ]
}
```

Sottoreti condivise

Un endpoint CloudTrail VPC, come qualsiasi altro endpoint VPC, può essere creato solo da un account proprietario nella sottorete condivisa. Tuttavia, un account partecipante può utilizzare gli endpoint CloudTrail VPC nelle sottoreti condivise con l'account del partecipante. Per ulteriori informazioni sulla condivisione di Amazon VPC, consulta Condivisione del VPC con altri account nella Guida per l'utente di Amazon VPC.

Requisiti di denominazione per CloudTrail risorse, bucket S3 e chiavi KMS

Questa sezione fornisce informazioni sui requisiti di denominazione per CloudTrail le risorse, i bucket Amazon S3 e le chiavi KMS.

Argomenti

- CloudTrail requisiti di denominazione delle risorse
- Requisiti di denominazione dei bucket Amazon S3
- AWS KMS requisiti di denominazione degli alias

CloudTrail requisiti di denominazione delle risorse

CloudTrail i nomi delle risorse devono soddisfare i seguenti requisiti:

- Contenere solo lettere ASCII (a-z, A-Z), numeri (0-9), punti (.), caratteri di sottolineatura (_) o trattini (-).
- Iniziare e terminare con una lettera o un numero.
- Contenere da 3 a 128 caratteri.
- Non contenere punti, caratteri di sottolineatura o trattini contigui. Nomi quali, ad esempio, my-_namespace e my-\-namespace non sono validi.
- Non devono usare il formato di indirizzo IP (ad esempio, `192.168.5.4`).

Requisiti di denominazione dei bucket Amazon S3

Il bucket Amazon S3 che usi per archiviare i file di CloudTrail log deve avere un nome conforme ai requisiti di denominazione per le regioni standard non statunitensi. Amazon S3 definisce un nome di bucket come una serie di una o più etichette, separate da punti. Per un elenco completo delle regole di denominazione, consulta Regole di denominazione dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

Di seguito sono elencate alcune regole:

- Il nome di bucket può essere include da 3 a 63 caratteri e contenere solo caratteri minuscoli, numeri, punti e trattini.
- Ogni etichetta nel nome di bucket deve iniziare con un numero o una lettera minuscola.
- Il nome di bucket non può contenere caratteri di sottolineatura, né terminare con un trattino, avere due punti consecutivi o utilizzare trattini accanto ai punti.
- Il nome di bucket non può avere il formato di un indirizzo IP (ad esempio, 198.51.100.24).

> **Warning**
>
> Poiché S3 supporta l'uso del bucket come URL a cui è possibile accedere pubblicamente, il nome di bucket selezionato deve essere univoco a livello globale. Se alcuni altri account hanno già creato un bucket con il nome scelto, devi utilizzare un altro nome. Per ulteriori informazioni, consulta Restrizioni e limitazioni dei bucket nella Guida per l'utente di Amazon Simple Storage Service.

AWS KMS requisiti di denominazione degli alias

Quando si crea un AWS KMS key, è possibile scegliere un alias per identificarlo. Ad esempio, puoi scegliere l'alias «KMS- CloudTrail -us-west-2" per crittografare i log di un percorso specifico.

L'alias deve soddisfare i seguenti requisiti:

- Contenere da 1 a 256 caratteri.
- Contenere caratteri alfanumerici (A-Z, a-z, 0-9), trattini (-), barre (/) e caratteri di sottolineatura (_).
- Non può iniziare con aws

Per ulteriori informazioni, consulta Creazione di chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Account AWS chiusura e percorsi

AWS CloudTrail monitora e registra continuamente gli eventi relativi all'attività dell'account generata da qualsiasi utente, ruolo o Servizio AWS per un Account AWS. Gli utenti possono creare un CloudTrail percorso per ricevere una copia di questi eventi in un bucket S3 di loro proprietà.

CloudTrail è un servizio di sicurezza fondamentale, pertanto, i percorsi creati dagli utenti continuano a esistere e forniscono eventi anche dopo la chiusura, a meno che un Account AWS utente non li elimini esplicitamente prima di chiuderlo. Account AWS In questo modo, se un utente riapre un account chiuso, dispone di un record ininterrotto delle attività dell'account. Inoltre, gli utenti potranno visualizzare qualsiasi attività finale dell'account, inclusa l'eliminazione e la chiusura delle risorse e dei servizi rimanenti.

Prima di chiudere il tuo Account AWS, considera quanto segue:

- I sentieri continuano ad esistere anche dopo la fine del periodo successivo alla chiusura. Il periodo successivo alla chiusura si riferisce ai 90 giorni che intercorrono tra la chiusura dell'account e la chiusura AWS definitiva del conto. Account AWS
- Questo comportamento si applica anche agli itinerari organizzativi creati dall'account di gestione o dall'amministratore delegato e agli itinerari organizzativi multiregionali creati negli account dei membri dell'organizzazione.
- Per i percorsi che inviano eventi a un bucket S3 nello stesso account, i percorsi continuano a esistere anche dopo la chiusura dell'account. Tuttavia, poiché il bucket S3 viene eliminato quando l'account viene chiuso, i trail non continuano a generare eventi.

- Per i percorsi che inviano eventi a un bucket S3 in un altro account, i trail continuano a esistere anche dopo la chiusura dell'account. I trail continuano inoltre a inviare eventi al bucket S3, se gli eventi possono essere distribuiti. Ad esempio, gli itinerari organizzativi continuano a inviare eventi al bucket S3 se si chiude un account membro in un'organizzazione, ma non si chiude l'account di gestione.
- Per i percorsi crittografati con AWS KMS keys, i trail continuano a esistere anche dopo la chiusura dell'account, oltre alle chiavi KMS.

Gli utenti hanno la possibilità di eliminare i percorsi prima di chiuderli Account AWS o di contattarci Supporto AWSper richiedere l'eliminazione dei percorsi dopo Account AWS la chiusura.

Per informazioni sulla chiusura di un Account AWS, consulta Close an Account AWS nella Guida Gestione dell'account AWS di riferimento.

> **Note**
>
> Se la convalida dei file di CloudTrail registro è abilitata, gli utenti continueranno a ricevere file digest con cadenza oraria che indicano se sono stati creati o meno CloudTrail registri. CloudTrail I data store di eventi Lake, i canali CloudTrail Lake per le integrazioni, i canali CloudTrail collegati ai servizi e le risorse create per i trail (ad esempio, i gruppi di log di Amazon CloudWatch Logs e i bucket Amazon S3 esistenti nell'account chiuso) seguono il AWS comportamento standard per la chiusura dell'account e vengono eliminati definitivamente dopo il periodo successivo alla chiusura (in genere 90 giorni).

Configurare CloudTrail le impostazioni

Puoi utilizzare la pagina Impostazioni sulla CloudTrail console per configurare e rivedere le CloudTrail impostazioni, ad esempio la gestione degli amministratori delegati di un' AWS Organizations organizzazione e la visualizzazione di tutti i canali collegati ai servizi creati per il tuo account.

Per accedere alla pagina Impostazioni

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra della CloudTrail console.
3. Rivedi e aggiorna le impostazioni in base alle necessità.

   Sono disponibili le impostazioni seguenti:

   - Amministratori delegati dell'organizzazione: se disponi di un' AWS Organizations organizzazione, puoi visualizzare gli amministratori CloudTrail delegati, aggiungere amministratori delegati (fino a un massimo di tre) e rimuovere gli amministratori delegati. Solo l'account di gestione dell'organizzazione può aggiungere o rimuovere amministratori delegati.

     L'account di gestione dell'organizzazione può assegnare a qualsiasi account all'interno dell'organizzazione il ruolo di amministratore CloudTrail delegato per gestire i percorsi e gli archivi di dati degli eventi dell'organizzazione per conto dell'organizzazione.
   - Visualizzazione dei canali collegati ai servizi— Puoi visualizzare tutti i canali collegati ai servizi creati per il tuo account.

     Servizi AWS può creare un canale collegato ai servizi per ricevere CloudTrail eventi per tuo conto. Il AWS servizio che crea il canale collegato al servizio configura selettori di eventi avanzati per il canale e specifica se il canale si applica a tutti o a uno solo. Regioni AWS Regione AWS

Amministratori delegati dell'organizzazione

Quando usi CloudTrail una AWS Organizations organizzazione, puoi assegnare qualsiasi account all'interno dell'organizzazione in modo che funzioni come amministratore CloudTrail delegato per gestire i trail e i datastore di eventi dell'organizzazione per conto dell'organizzazione stessa. Un

amministratore delegato è un account membro di un'organizzazione che può eseguire le stesse attività amministrative (tranne dove riportato) dell'account di gestione. CloudTrail

Se scegli un amministratore delegato, questo account membro disporrà di autorizzazioni amministrative su tutti i percorsi e i datastore di eventi dell'organizzazione. L'aggiunta di un amministratore delegato non interrompe la gestione o il funzionamento dei percorsi o dei datastore di eventi dell'organizzazione.

La prima volta che aggiungi un amministratore delegato nella CloudTrail console, oppure utilizzando l' AWS CLI o CloudTrail API, CloudTrail verifica che l'account di gestione dell'organizzazione abbia un ruolo collegato al servizio. Se l'account di gestione non ha un ruolo collegato al servizio, CloudTrail crea il ruolo collegato al servizio per l'account di gestione. Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per CloudTrail.

> **Note**
>
> Quando aggiungi un amministratore delegato utilizzando la o l' AWS Organizations operazione API CloudTrail , i ruoli collegati al servizio non verranno creati automaticamente se non esistono. I ruoli collegati al servizio vengono creati solo quando si effettua una chiamata dall'account di gestione direttamente al servizio. CloudTrail Ad esempio, quando aggiungi un amministratore delegato o crei un percorso dell'organizzazione o un datastore di eventi utilizzando la CloudTrail console AWS CLI o l' CloudTrail API, viene creato il ruolo AWSServiceRoleForCloudTrail collegato al servizio.
> Quando aggiungi un amministratore delegato utilizzando l'operazione AWS CloudTrail; CLI o API CloudTrail , creerà sia AWSServiceRoleForCloudTrail il ruolo che il ruolo collegato al servizio. AWSServiceRoleForCloudTrailEventContext Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per CloudTrail..

Prendi nota dei seguenti fattori che definiscono il modo in cui l'amministratore delegato opera in CloudTrail.

L'account di gestione rimane il proprietario di tutte le risorse CloudTrail dell'organizzazione create dall'amministratore delegato.

> L'account di gestione rimane il proprietario di tutte le risorse CloudTrail dell'organizzazione create dall'amministratore delegato, come ad esempio trail ed datastore di eventi. Ciò garantisce continuità all'organizzazione nel caso in cui l'amministratore delegato cambi.

Rimozione di un account amministratore delegato non comporta l'eliminazione delle risorse CloudTrail dell'organizzazione create.

> I trail dell'organizzazione e i datastore di eventi creati dall'amministratore delegato non vengono eliminati quando si rimuove l'amministratore delegato, poiché l'account di gestione funge sempre da proprietario delle risorse dell' CloudTrail organizzazione, indipendentemente dal fatto che siano state create dall'amministratore delegato o dall'account di gestione.

Un'organizzazione può avere un massimo di tre amministratori CloudTrail delegati.

> Puoi avere un massimo di tre amministratori CloudTrail delegati per organizzazione. Per ulteriori informazioni sulla rimozione di un amministratore delegato, consulta Rimozione di un CloudTrail amministratore delegato.

Di seguito è riportata una tabella che mostra le funzionalità dell'account di gestione, degli account amministratore delegato e degli account che fanno parte dell' AWS Organizations organizzazione.

Funzionalità	Gestione dell'account	Account amministratore delegato	Account membri
Aggiunta o rimozione di account amministratore delegato.	Sì	No	No
Creazione di un percorso dell'organizzazione.	Sì	Sì [1]	No
Visualizzazione di un elenco dei percorsi dell'organizzazione.	Sì	Sì	Sì
Aggiornamento di un percorso dell'organizzazione.	Sì	S [1, 2]	No
Eliminazione di un percorso dell'organizzazione.	Sì	Sì	No
Creazione di un datastore di CloudTrail eventi per eventi o	Sì	Sì	No

Funzionalità	Gestione dell'account	Account amministratore delegato	Account membri
elementi AWS Config di configura zione.			
Abilitazione di Insights in un datastore di eventi dell'organizzazion e.	Sì	No	No
Aggiornamento di un datastore di eventi dell'organizzazione.	Sì	S [2]	No
Avvio e interruzione dell'inserimento di eventi in un datastore di eventi dell'organizzazione.	Sì	Sì	No
Abilitazione della federazione delle query di Data Lake in un datastore di eventi dell'organizzazione[3].	Sì	Sì	No
Disabilitazione della federazio ne delle query di Data Lake in un datastore di eventi dell'organizzazion e.	Sì	Sì	No
Eliminazione di un datastore di eventi dell'organizzazione.	Sì	Sì	No
Copia di eventi di percorso in un datastore di eventi dell'organizzazion e.	Sì	No	No
Esecuzione di query sui datastore di eventi dell'organizzazione.	Sì	Sì	No

Funzionalità	Gestione dell'account	Account amministratore delegato	Account membri
Visualizzazione di un pannello di controllo gestito per un datastore di eventi dell'organizzazione.	Sì	No	No
Abilitazione del pannello di controllo Highlights per datastore di eventi dell'organizzazione.	Sì	No	No
Creazione di un widget per un pannello di controllo personalizzato che interroga un datastore di eventi dell'organizzazione.	Sì	No	No

[1] L'amministratore delegato può configurare un gruppo di log CloudWatch Logs solo utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API. Nell'account chiamante devono essere presenti sia il gruppo di log che il ruolo di log CloudWatch Logs.

[2] Solo l'account di gestione può convertire un percorso dell'organizzazione o un datastore di eventi in un percorso o un datastore di eventi a livello di account, e viceversa. Queste azioni non sono consentite all'amministratore delegato perché i percorsi organizzativi e i datastore di eventi esistono solo nell'account di gestione. Quando un percorso dell'organizzazione o un datastore di eventi viene convertito in un percorso o in un datastore di eventi a livello di account, solo l'account di gestione ha accesso al percorso o al datastore.

[3]Solo un singolo account amministratore delegato o l'account di gestione può abilitare la federazione in un datastore di eventi dell'organizzazione. Altri account amministratore delegato possono eseguire query e condividere informazioni utilizzando la funzionalità di condivisione dei dati di Lake Formation. Qualsiasi account amministratore delegato, nonché l'account di gestione dell'organizzazione, può disabilitare la federazione.

Argomenti

- Autorizzazioni necessarie per assegnare un amministratore delegato
- Aggiunta di un CloudTrail amministratore delegato

- Rimozione di un CloudTrail amministratore delegato

Autorizzazioni necessarie per assegnare un amministratore delegato

Quando assegni un amministratore CloudTrail delegato, devi disporre delle autorizzazioni per aggiungere e rimuovere l'amministratore delegato CloudTrail, nonché di alcune operazioni AWS Organizations API e autorizzazioni IAM elencate nella seguente istruzione di policy.

Puoi aggiungere la seguente istruzione alla fine di una policy IAM esistente per concedere queste autorizzazioni:

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

Considerazioni sull'utilizzo delle chiavi condizionali con le dichiarazioni delle politiche per le autorizzazioni di amministratore delegato

Potresti prendere in considerazione l'utilizzo delle chiavi di condizione globali IAM quando aggiungi dichiarazioni di policy per aggiungere e rimuovere l'amministratore delegato CloudTrail per una maggiore sicurezza. Quando lo fai, ricorda di includere entrambi i nomi principali dei servizi (SPNs) nella condizione. Per esempio:

```
{
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "context.cloudtrail.amazonaws.com",
            "cloudtrail.amazonaws.com"
```

```
            ]
          }
        },
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Effect": "Allow"
}
```

Per ulteriori informazioni, consulta Identity and Access Management per AWS CloudTrail.

Aggiunta di un CloudTrail amministratore delegato

Puoi aggiungere un amministratore delegato per gestire le CloudTrail risorse di un'organizzazione, come trail ed datastore di eventi.

È possibile aggiungere un amministratore CloudTrail delegato per l' AWS organizzazione utilizzando la CloudTrail console o il. AWS CLI

Prima di aggiungere un amministratore delegato, assicurati che disponga di un account nella tua organizzazione e di aver effettuato l'accesso con l'account di gestione della tua organizzazione. Per informazioni su come creare un nuovo AWS account per la tua organizzazione, consulta Creazione di un AWS account nell'organizzazione. Per informazioni su come invitare un AWS account esistente a entrare in un'organizzazione, consulta Invito di un AWS account a far parte di un'organizzazione.

CloudTrail console

Nella procedura seguente viene illustrato come aggiungere un amministratore CloudTrail delegato utilizzando la CloudTrail console.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra della CloudTrail console, scegli Settings (Impostazioni).
3. Nella sezione Organization delegated administrators (Amministratori delegati dell'organizzazione), scegli Register administrator (Registra amministratore).
4. Immetti l'ID AWS account a 12 cifre dell'account che si desidera designare come amministratore CloudTrail delegato per i trail e i datastore di eventi dell'organizzazione.
5. Scegli Register administrator (Registra amministratore).

AWS CLI

L'esempio seguente aggiunge un amministratore CloudTrail delegato.

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

Se ha esito positivo, questo comando non produrrà alcun output.

Rimozione di un CloudTrail amministratore delegato

Puoi rimuovere un amministratore CloudTrail delegato utilizzando la CloudTrail console o la AWS CLI.

CloudTrail console

Nella procedura seguente viene illustrato come rimuovere un amministratore CloudTrail delegato utilizzando la CloudTrail console.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra della CloudTrail console, scegli Settings (Impostazioni).
3. Nella sezione Organization delegated administrators (Amministratori delegati dell'organizzazione), scegli l'amministratore delegato che desideri rimuovere.
4. Scegli Remove administrator (Rimuovi amministratore).
5. Conferma di voler rimuovere l'amministratore delegato, quindi scegli Remove administrator (Rimuovi amministratore).

AWS CLI

L'esempio seguente rimuove un amministratore CloudTrail delegato.

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

Se ha esito positivo, questo comando non produrrà alcun output.

Visualizzazione dei canali collegati ai servizi

AWS i servizi possono creare un canale collegato al servizio per ricevere CloudTrail eventi per tuo conto. Il AWS servizio che crea il canale collegato al servizio configura selettori di eventi avanzati per il canale e specifica se il canale si applica a tutti o a uno solo. Regioni AWS Regione AWS

Argomenti

- Visualizzazione di canali collegati ai servizi tramite la console
- Visualizzazione dei canali collegati al servizio utilizzando il AWS CLI

Visualizzazione di canali collegati ai servizi tramite la console

Utilizzando la CloudTrail console, è possibile visualizzare informazioni su tutti i canali collegati ai servizi creati dai CloudTrail servizi. AWS La tabella è vuota se l'account non dispone di canali collegati al servizio.

Utilizzare la procedura seguente per visualizzare le informazioni su un canale collegato al servizio.

1. Scegli Impostazioni nel riquadro di navigazione a sinistra della CloudTrail console.
2. Da Canali collegati ai servizi, scegli un canale collegato al servizio per visualizzarne i dettagli.
3. Nella pagina dei dettagli, rivedi le impostazioni configurate per il canale collegato al servizio.

   Nella pagina dei dettagli è possibile visualizzare le seguenti informazioni.

   - Nome canale: il nome completo del canale. Il formato del nome del canale è `aws-service-channel/`*`AWS_service_name`*`/slc` dove *`AWS_service_name`* rappresenta il nome del AWS servizio che gestisce il canale.
   - ARN del canale: l'ARN del canale, che puoi utilizzare in una richiesta API per ottenere dettagli sul canale.
   - Tutte le regioni: il valore è `Yes` se il canale è configurato per tutte le Regioni AWS.
   - AWS service - Il nome del AWS servizio che gestisce il canale.
   - Eventi di gestione: mostra tutti gli eventi di gestione configurati per il canale.
   - Eventi di dati: mostra tutti gli eventi relativi ai dati configurati per il canale.

Visualizzazione dei canali collegati al servizio utilizzando il AWS CLI

Utilizzando AWS CLI, è possibile visualizzare informazioni su tutti i canali CloudTrail collegati ai servizi creati dai servizi. AWS

Argomenti

- Ottieni un canale collegato ai servizi CloudTrail
- Elenca tutti i CloudTrail canali collegati al servizio
- AWS eventi di servizio sui canali collegati al servizio

Ottieni un canale collegato ai servizi CloudTrail

Il AWS CLI comando di esempio seguente restituisce informazioni su uno specifico canale CloudTrail collegato al servizio, incluso il nome del AWS servizio di destinazione, eventuali selettori avanzati configurati per il canale e se il canale si applica a tutte le regioni o a una singola regione.

Devi specificare un ARN o il suffisso ID di un ARN per `--channel`.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

Di seguito è riportata una risposta di esempio. In questo esempio, `AWS_service_name` rappresenta il nome del AWS servizio che ha creato il canale.

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
```

```
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

Elenca tutti i CloudTrail canali collegati al servizio

Il AWS CLI comando di esempio seguente restituisce informazioni su tutti i canali CloudTrail collegati ai servizi che sono stati creati per conto dell'utente. I parametri opzionali includono `--max-results`, che consente di specificare il numero massimo di risultati che desideri che il comando restituisca su una singola pagina. Se ci sono più risultati di quanto specificato dal valore `--max-results`, esegui nuovamente il comando aggiungendo il valore `NextToken` restituito per visualizzare la pagina dei risultati successiva.

```
aws cloudtrail list-channels
```

Di seguito è riportata una risposta di esempio. In questo esempio, `AWS_service_name` rappresenta il nome del AWS servizio che ha creato il canale.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS eventi di servizio sui canali collegati al servizio

Il AWS servizio che gestisce il canale collegato al servizio può avviare azioni sul canale collegato al servizio (ad esempio, la creazione o l'aggiornamento di un canale collegato al servizio). CloudTrail registra queste azioni come eventi di AWS servizio e li inserisce nella cronologia degli eventi e in tutti gli itinerari attivi e gli archivi dati degli eventi configurati per gli eventi di gestione. Per questi eventi, il campo `eventType` è `AwsServiceEvent`.

Di seguito è riportato un esempio di immissione nel file di registro di un evento di AWS servizio per la creazione di un canale collegato al servizio.

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

Comprendere CloudTrail gli eventi

Un evento in CloudTrail è la registrazione di un'attività in un AWS account. Questa attività può essere un'azione intrapresa da un'identità IAM o da un servizio monitorabile da CloudTrail. CloudTrail gli eventi forniscono una cronologia delle attività dell'account API e non API effettuate tramite gli AWS Management Console strumenti a riga di comando e altro. AWS SDKs Servizi AWS

CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

Esistono quattro tipi di CloudTrail eventi:

- Eventi di gestione
- Eventi di dati
- Eventi di attività di rete
- Eventi di approfondimento

Per impostazione predefinita, i percorsi e i dati degli eventi registrano gli eventi di gestione, ma non gli eventi relativi ai dati, gli eventi delle attività di rete o gli eventi Insights.

Tutti i tipi di eventi utilizzano un formato di registro CloudTrail JSON. Il log contiene informazioni sulle richieste di risorse a livello di account, ad esempio l'utente che ha effettuato la richiesta, i servizi utilizzati, le azioni eseguite e i parametri dell'operazione. I dati relativi agli eventi sono racchiusi in una matrice `Records`.

Per informazioni sui campi di registrazione CloudTrail degli eventi per gli eventi di gestione, dati e attività di rete, consultaCloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

Per informazioni sui campi di registrazione degli CloudTrail eventi per gli eventi Insights per i percorsi, vedereCloudTrail registra contenuti per gli eventi Insights per i percorsi.

Per informazioni sui campi di registrazione CloudTrail degli eventi per gli eventi di Insights per gli archivi dati degli eventi, vedereCloudTrail registra i contenuti per gli eventi Insights per i datastore di eventi Lake..

Eventi di gestione

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse AWS dell'account. Queste operazioni sono definite anche operazioni del piano di controllo.

Gli eventi di gestione di esempio includono:

- Configurazione della sicurezza (ad esempio, operazioni AWS Identity and Access Management `AttachRolePolicy` API).
- Registrazione di dispositivi (ad esempio, operazioni EC2 `CreateDefaultVpc` API Amazon).
- Configurazione delle regole per il routing dei dati (ad esempio, le operazioni delle EC2 `CreateSubnet` API Amazon).
- Configurazione della registrazione (ad esempio, operazioni AWS CloudTrail `CreateTrail` API).

Gli eventi di gestione possono includere anche eventi non API che si verificano nel tuo account. Ad esempio, quando un utente accede al tuo account, CloudTrail registra l'`ConsoleLogin`evento. Per ulteriori informazioni, consulta Eventi non API acquisiti da CloudTrail.

Per impostazione predefinita, CloudTrail trails and CloudTrail Lake Event Data archivia gli eventi di gestione dei registri. Per ulteriori informazioni sulla gestione della registrazione degli eventi, vedereRegistrazione degli eventi di gestione.

L'esempio seguente mostra un singolo record di registro di un evento di gestione. In questo caso, un utente IAM denominato `Mary_Major` ha eseguito il aws cloudtrail start-logging comando per richiamare l' CloudTrail `StartLogging`azione di avvio del processo di registrazione su un percorso denominato`myTrail`.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

In questo esempio successivo, un utente IAM di nome `Paulo_Santos` ha eseguito il comando aws cloudtrail start-event-data-store-ingestion per richiamare l'operazione `StartEventDataStoreIngestion` per avviare l'importazione su un datastore di eventi.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
```

```
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Eventi di dati

Gli eventi di dati forniscono informazioni sulle operazioni eseguite in una risorsa o al suo interno. Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati.

Gli eventi di dati di esempio includono:

- Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject``DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket S3.
- AWS Lambda attività di esecuzione della funzione (l'API). `Invoke`
- CloudTrail `PutAuditEvents`attività su un canale CloudTrail Lake che viene utilizzata per registrare eventi dall'esterno AWS.
- Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.

La tabella seguente mostra i tipi di risorse disponibili per i percorsi e gli archivi di dati di eventi. La colonna Tipo di risorsa (console) mostra la selezione appropriata nella console. La colonna del valore resources.type mostra il `resources.type` valore da specificare per includere eventi di dati di quel tipo nel tuo trail o event data store utilizzando o. AWS CLI CloudTrail APIs

Per i trail, puoi utilizzare selettori di eventi di base o avanzati per registrare gli eventi di dati per oggetti Amazon S3 in bucket generici, funzioni Lambda e tabelle DynamoDB (mostrate nelle prime tre righe della tabella). Puoi utilizzare solo selettori di eventi avanzati per registrare i tipi di risorse mostrati nelle righe rimanenti.

Per i datastore di eventi, per includere gli eventi di dati è possibile utilizzare solo i selettori di eventi avanzati.

Eventi di dati supportati da AWS CloudTrail

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Backup	AWS Backup Attività dell'API Search Data sui lavori di ricerca.	AWS Backup Dati di ricerca APIs	`AWS::Backup::SearchJob`
AWS IoT	AWS IoT Attività delle API sui certificati.	Certificato IoT	`AWS::IoT::Certificate`
AWS IoT	AWS IoT Attività delle API sugli oggetti.	Cosa IoT	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Connettore per l'attivit	AWS Private CA Connettor	`AWS::PCAConnectorAD::Connector`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
	à dell'API di Active Directory.	e per Active Directory	
AWS Private CA	AWS Private CA Connettore per l'attivit à dell'API SCEP.	AWS Private CA Connettor e per SCEP	`AWS::PCAConnectorSCEP::Connector`
Amazon RDS	Attività dell'API Amazon RDS su un cluster DB.	API dati RDS - Cluster DB	`AWS::RDS::DBCluster`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject`, e operazioni `PutObject` API) su oggetti in bucket generici.	S3	`AWS::S3::Object`
Amazon S3	Attività dell'API Amazon S3 sui punti di accesso.	Punto di accesso S3	`AWS::S3::AccessPoint`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket di directory.	S3 Express	`AWS::S3Express::Object`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon S3	Attività delle API dei punti di accesso Amazon S3 Object Lambda, ad esempio chiamate a e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	Attività FSx delle API Amazon sui volumi.	FSx Volume	`AWS::FSx::Volume`
Tabelle di Amazon S3	Attività dell'API Amazon S3 sulle tabelle.	Tabella S3	`AWS::S3Tables::Table`
Tabelle di Amazon S3	Attività dell'API Amazon S3 su bucket da tabella.	Secchio da tavolo S3	`AWS::S3Tables::TableBucket`
Amazon S3 su Outposts	Attività dell'API a livello di oggetto di Amazon S3 su Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SNS	Operazioni dell'API `Publish` Amazon SNS sugli endpoint della piattaforma.	Endpoint della piattaforma SNS	`AWS::SNS::PlatformEndpoint`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon SNS	Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.	Argomento SNS	`AWS::SNS::Topic`
Amazon SQS	Attività dell'API Amazon SQS sui messaggi.	SQS	`AWS::SQS::Queue`
Catena di approvvigionamento di AWS	Catena di approvvigionamento di AWS Attività dell'API su un'istanza.	Catena di fornitura	`AWS::SCN::Instance`
Amazon SWF	Attività dell'API Amazon SWF sui domini.	Dominio SWF	`AWS::SWF::Domain`
AWS AppConfig	AWS AppConfig Attività dell'API per operazioni di configurazione come chiamate a `StartConfigurationSessioneGetLatestConfiguration`.	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AWS AppSync Attività delle API su AppSync GraphQL APIs.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Aurora DSQL	Attività dell'API SQL di Amazon Aurora sulle risorse del cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
AWS Scambio di dati B2B	Attività dell'API Scambio di dati B2B per operazioni Transformer, come le chiamate a `GetTransformerJob` e `StartTransformerJob` .	Scambio di dati B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Attività dell'API Amazon Bedrock sull'alias di un agente.	Alias dell'agente Bedrock	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle chiamate asincrone.	Richiamo asincrono Bedrock	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	Attività dell'API Amazon Bedrock su un alias di flusso.	Alias di flusso Bedrock	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui guardrail.	Parapetto Bedrock	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Attività dell'API Amazon Bedrock sugli agenti in linea.	Agente in linea Bedrock Invoke	`AWS::Bedrock::InlineAgent`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Bedrock	Attività dell'API Amazon Bedrock su una knowledge base.	Knowledge base Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui modelli.	Modello Bedrock	`AWS::Bedrock::Model`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui prompt.	Richiesta Bedrock	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	Attività dell'API Amazon Bedrock nelle sessioni.	Sessione Bedrock	`AWS::Bedrock::Session`
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle esecuzioni dei flussi.	Esecuzione del flusso di base	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una politica di ragionamento automatico.	Politica di ragionamento automatizzato di base	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una versione di policy di ragionamento automatico.	Versione della politica di ragionamento automatico Bedrock	`AWS::Bedrock::AutomatedReasoningPolicyVersion`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Cloud Map	AWS Cloud Map Attività dell'API su un namespace.	AWS Cloud Map spazio dei nomi	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	AWS Cloud Map Attività dell'API su un servizio.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	CloudFront Attività API su un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS CloudTrail	CloudTrail `PutAuditEvents` attività su un canale CloudTrail Lake che viene utilizzato per registrare eventi dall'esterno AWS.	CloudTrail canale	`AWS::CloudTrail::Channel`
Amazon CloudWatch	Attività dell' CloudWatch API Amazon sulle metriche.	CloudWatch parametro	`AWS::CloudWatch::Metric`
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sui monitor.	Monitor di Network Flow Monitor	`AWS::NetworkFlowMonitor::Monitor`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sugli ambiti.	Ambito di Network Flow Monitor	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	Attività dell'API Amazon CloudWatch RUM sui monitor delle app.	Monitoraggio delle app RUM	`AWS::RUM::AppMonitor`
Amazon CodeGuru Profiler	CodeGuru Attività dell'API Profiler sui gruppi di profilazione.	CodeGuru Gruppo di profilazione Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su una personalizzazione.	CodeWhisperer personalizzazione	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su un profilo.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Attività dell'API Amazon Cognito sui pool di identità di Amazon Cognito.	Pool di identità di Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange Attività delle API sugli asset.	Risorsa Data Exchange	`AWS::DataExchange::Asset`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Deadline Cloud	Deadline CloudAttività delle API sulle flotte.	Deadline Cloud flotta	`AWS::Deadline::Fleet`
AWS Deadline Cloud	Deadline Cloudattività delle API sui lavori.	Deadline Cloud lavoro	`AWS::Deadline::Job`
AWS Deadline Cloud	Deadline Cloudattività delle API in coda.	Deadline Cloud coda	`AWS::Deadline::Queue`
AWS Deadline Cloud	Deadline CloudAttività delle API sui lavoratori.	Deadline Cloud lavoratore	`AWS::Deadline::Worker`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon DynamoDB	Attività delle API a livello di elemento di Amazon DynamoDB sulle tabelle (ad esempio `PutItem`, `DeleteItem` e operazioni API). `UpdateItem` **Note** Per le tabelle con flussi abilitati, il campo `resources` nell'evento di dati contiene sia `AWS::DynamoDB::Stream` che `AWS::DynamoDB::Table`. Se specifichi `AWS::DynamoDB::Table` come `resources.type`, per impostazione predefini	DynamoDB	`AWS::DynamoDB::Table`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
	ta verranno registrati sia gli eventi della tabella DynamoDB che quelli dei flussi DynamoDB. Per escludere gli eventi di streaming, aggiungi un filtro sul campo. `eventName`		
Amazon DynamoDB	Attività dell'API Amazon DynamoDB sui flussi	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct APIs, ad esempio `GetSnapshotBlock` e su `PutSnapshotBlock` istantanee e `ListChangedBlocks` Amazon EBS.	Amazon EBS diretto APIs	`AWS::EC2::Snapshot`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Elastic Kubernetes Service	Attività dell'API Amazon Elastic Kubernetes Service sulle dashboard.	Pannello di controllo di Amazon Elastic Kubernetes Service	`AWS::EKS::Dashboard`
Amazon EMR	Attività dell'API Amazon EMR su un'area di lavoro di log write-ahead.	Workspace di registrazione write-ahead EMR	`AWS::EMRWAL::Workspace`
AWS Messaggistica per l'utente finale (SMS)	AWS Attività dell'API SMS di messaggistica per l'utente finale sulle identità di origine.	Identità di origine tramite SMS Voice	`AWS::SMSVoice::OriginationIdentity`
AWS SMS di messaggistica per l'utente finale	AWS Attività dell'API SMS di messaggistica per l'utente finale sui messaggi.	Messaggio vocale SMS	`AWS::SMSVoice::Message`
AWS Messaggistica sociale per utenti finali	AWS Attività dell'API Social Messaging per l'utente finale sul numero di telefono IDs.	ID del numero di telefono di messaggistica sociale	`AWS::SocialMessaging::PhoneNumberId`
AWS Social di messaggistica per utenti finali	AWS Attività dell'API End User Messaging Social su Waba IDs.	ID Waba per la messaggistica sociale	`AWS::SocialMessaging::WabaId`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon FinSpace	Attività dell'API Amazon FinSpace sugli ambienti	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Stream	L'attività delle API di streaming di Amazon GameLift Streams sulle applicazioni.	GameLift Applicazione Streams	`AWS::GameLiftStreams::Application`
Amazon GameLift Stream	Attività delle API di streaming di Amazon GameLift Streams sui gruppi di stream.	GameLift Gruppo di stream Streams	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Attività dell'API su tabelle create da Lake Formation.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	Attività dell' GuardDuty API Amazon per un rilevatore.	GuardDuty rilevatore	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging attività delle API sugli archivi dati.	MedicalImaging archivio dati	`AWS::MedicalImaging::Datastore`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass su una versione componente. **Note** Greengrass non registra gli eventi di accesso negato.	Versione componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass in una distribuzione. **Note** Greengrass non registra gli eventi di accesso negato.	Implementazione di IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Attività dell' SiteWise API IoT sugli asset.	SiteWise Risorsa IoT	`AWS::IoTSiteWise::Asset`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT SiteWise	Attività dell' SiteWise API IoT su serie temporali.	Serie SiteWise temporali IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT SiteWise Assistente	Attività dell'API Sitewise Assistant sulle conversazioni.	Conversazione con Sitewise Assistant	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'entità.	TwinMaker Entità IoT	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'area di lavoro.	Spazio di TwinMaker lavoro IoT	`AWS::IoTTwinMaker::Workspace`
Classificazione intelligente di Amazon Kendra	Attività dell'API Amazon Kendra Intelligent Ranking sui piani di esecuzione di rescore.	Classificazione Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces su una tabella.	Tabella Cassandra	`AWS::Cassandra::Table`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces (per Apache Cassandra) sugli stream Cassandra CDC.	Stream Cassandra CDC	`AWS::Cassandra::Stream`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sugli stream.	Stream Kinesis	`AWS::Kinesis::Stream`
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sui consumatori di streaming.	Kinesis Stream Consumer	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Attività dell'API Kinesis Video Streams sui flussi video, ad esempio chiamate verso e. `GetMedia` `PutMedia`	Flusso video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda attività di esecuzione delle funzioni (l'API). `Invoke`	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Attività dell'API Amazon Location Maps.	Mappe geografiche	`AWS::GeoMaps::Provider`
Luoghi di Amazon Location	Attività dell'API Amazon Location Places.	Luoghi geografici	`AWS::GeoPlaces::Provider`
Route di Amazon Location	Attività dell'API Amazon Location Routes.	Percorsi geografici	`AWS::GeoRoutes::Provider`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Machine Learning	Attività dell'API di Machine Learning sui modelli ML.	Apprendimento automatico MlModel	`AWS::MachineLearning::MlModel`
Blockchain gestita da Amazon	Attività dell'API Blockchain gestita da Amazon su una rete.	Rete Blockchain gestita	`AWS::ManagedBlockchain::Network`
Blockchain gestita da Amazon	Chiamate JSON-RPC di Blockchain gestita da Amazon sui nodi Ethereum, come `eth_getBalance` o `eth_getBlockByNumber` .	Blockchain gestita	`AWS::ManagedBlockchain::Node`
Query su Blockchain gestita da Amazon	Attività dell'API Amazon Managed Blockchain Query.	Query Blockchain gestita	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	Attività dell'API Amazon MWAA negli ambienti.	Apache Airflow gestito	`AWS::MWAA::Environment`
Grafo Amazon Neptune	Attività dell'API dati, ad esempio query, algoritmi o ricerca vettoriale, su un grafo Neptune.	Grafo Neptune	`AWS::NeptuneGraph::Graph`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon One Enterprise	Attività dell'API Amazon One Enterprise su un UKey.	Amazon Uno UKey	`AWS::One::UKey`
Amazon One Enterprise	Attività dell'API Amazon One Enterprise sugli utenti.	Utente Amazon One	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sugli alias.	Alias di crittografia dei pagamenti	`AWS::PaymentCryptography::Alias`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sulle chiavi.	Chiave di crittografia dei pagamenti	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	Attività dell'API Amazon Pinpoint su applicazioni di targeting per dispositivi mobili.	Applicazione di targeting mobile	`AWS::Pinpoint::App`
App Amazon Q	Attività delle API di dati su Amazon Q Apps.	App Amazon Q	`AWS::QApps::QApp`
App Amazon Q	Attività delle API di dati nelle sessioni di Amazon Q App.	Sessione dell'app Amazon Q	`AWS::QApps::QAppSession`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Q Business	Attività dell'API Amazon Q Business su un'applicazione.	Applicazione Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Business	Attività dell'API Amazon Q Business su un'origine dati.	Origine dati Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Business	Attività dell'API Amazon Q Business su un indice.	Indice Amazon Q Business	`AWS::QBusiness::Index`
Amazon Q Business	Attività dell'API Amazon Q Business su un'esperienza Web.	Esperienza Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Attività dell'API Amazon Q Developer su un'integrazione.	Integrazione con Q Developer	`AWS::QDeveloper::Integration`
Amazon Q Developer	Attività dell'API Amazon Q Developer sulle indagini operative.	AIOps Gruppo di indagine	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	`InvokeEndpointWithResponseStream` Attività di Amazon SageMaker AI sugli endpoint.	SageMaker Endpoint AI	`AWS::SageMaker::Endpoint`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui feature store.	SageMaker AI feature store	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui componenti di prova sperimentali.	SageMaker Component e di prova dell'esperimento AI Metrics	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	Attività dell'API Signer sulla firma dei lavori.	Firmatario che firma un lavoro	`AWS::Signer::SigningJob`
AWS Signer	Attività dell'API Signer sulla firma dei profili.	Profilo di firma del firmatario	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui set di configurazione.	Set di configurazione SES	`AWS::SES::ConfigurationSet`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sulle identità e-mail.	Identità SES	`AWS::SES::EmailIdentity`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui modelli.	Modello SES	`AWS::SES::Template`
Amazon SimpleDB	Attività dell'API Amazon SimpleDB sui domini.	Dominio SimpleDB	`AWS::SDB::Domain`
AWS Step Functions	Attività dell'API Step Functions sulle attività.	Step Functions	`AWS::StepFunctions::Activity`
AWS Step Functions	Attività dell'API Step Functions su macchine a stati.	Macchina a stati di Step Functions	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	Attività dell'API Systems Manager sui canali di controllo.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	Attività dell'API Systems Manager sulle valutazioni dell'impatto.	Valutazione dell'impatto SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Attività dell'API Systems Manager sui nodi gestiti.	Nodo gestito da Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sui database.	Database Timestream	`AWS::Timestream::Database`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Timestream	Attività dell'API Amazon Timestream sugli endpoint regionali.	Endpoint regionale Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sulle tabelle.	Tabella Timestream	`AWS::Timestream::Table`
Autorizzazioni verificate da Amazon	Attività dell'API Autorizzazioni verificate da Amazon su un archivio di policy.	Autorizzazioni verificate da Amazon	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client su un dispositivo.	Dispositivo Thin client	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client in un ambiente.	Ambiente Thin client	`AWS::ThinClient::Environment`
AWS X-Ray	Attività dell'API X-Ray sulle tracce.	Traccia a raggi X	`AWS::XRay::Trace`

Quando si crea un percorso o un datastore di eventi, gli eventi di dati non vengono registrati per impostazione predefinita. Per registrare gli eventi CloudTrail relativi ai dati, è necessario aggiungere in modo esplicito le risorse o i tipi di risorse supportati per i quali si desidera raccogliere attività. Per ulteriori informazioni, consultare Creazione di un percorso con la CloudTrail console e Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per CloudTrail i prezzi, consulta AWS CloudTrail Prezzi.

L'esempio seguente mostra un singolo record di log di un evento di dati per l'azione Amazon `SNSPublish`.


```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
```

```
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

L'esempio successivo mostra un singolo record di log di un evento di dati per l'azione Amazon Cognito`GetCredentialsForIdentity`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
```

```
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

Eventi di attività di rete

CloudTrail gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Gli eventi di attività di rete forniscono visibilità sulle operazioni sulle risorse eseguite all'interno di un VPC.

È possibile registrare gli eventi di attività di rete per i seguenti servizi:

- AWS AppConfig
- AWS B2B Data Interchange
- Gestione dei costi e fatturazione
- Calcolatore dei prezzi AWS
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail

- Esportazioni di dati AWS
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EventBridge Scheduler
- Piano gratuito di AWS
- Amazon FSx
- AWS IoT FleetWise
- Fatturazione AWS
- AWS KMS
- AWS Lambda
- Amazon Lookout per le apparecchiature
- Amazon Rekognition
- Amazon S3

> **Note**
>
> Gli access point multiregionali di Amazon S3 non sono supportati.

- AWS Secrets Manager
- Strumento di gestione degli incidenti AWS Systems Manager
- Amazon Textract
- Amazon WorkMail

Per impostazione predefinita, gli eventi relativi alle attività di rete non vengono registrati quando si crea un archivio dati di percorsi o eventi. Per registrare gli eventi CloudTrail di attività di rete, è necessario impostare in modo esplicito l'origine dell'evento per cui si desidera raccogliere l'attività. Per ulteriori informazioni, consulta Registrazione degli eventi delle attività di rete.

Si applicano costi aggiuntivi per la registrazione degli eventi di attività di rete. Per CloudTrail informazioni sui prezzi, consulta la sezione AWS CloudTrail Prezzi.

L'esempio seguente mostra un AWS KMS `ListKeys` evento riuscito che ha attraversato un endpoint VPC. Il `vpcEndpointId` campo mostra l'ID dell'endpoint VPC. Il `vpcEndpointAccountId` campo

mostra l'ID dell'account del proprietario dell'endpoint VPC. In questo esempio, la richiesta è stata effettuata dal proprietario dell'endpoint VPC.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE:role-name",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/role-name",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-06-04T23:10:46Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-06-04T23:12:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "requestID": "16bcc089-ac49-43f1-9177-EXAMPLE23731",
    "eventID": "228ca3c8-5f95-4a8a-9732-EXAMPLE60ed9",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "a1f3720c-ef19-47e9-a5d5-EXAMPLE8099f",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```


L'esempio successivo mostra un AWS KMS `ListKeys` evento non riuscito con una violazione della policy degli endpoint VPC. Poiché si è verificata una violazione della policy VPC, sono presenti sia

i campi che `errorCode` i `errorMessage` campi. L'ID dell'account nei `vpcEndpointAccountId` campi `recipientAccountId` and è lo stesso, il che indica che l'evento è stato inviato al proprietario dell'endpoint VPC. L'`userIdentity`elemento `accountId` in the non è il`vpcEndpointAccountId`, il che indica che l'utente che effettua la richiesta non è il proprietario dell'endpoint VPC.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "777788889999"
    },
    "eventTime": "2024-07-15T23:57:12Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "errorCode": "VpceAccessDenied",
    "errorMessage": "The request was denied due to a VPC endpoint policy",
    "requestID": "899003b8-abc4-42bb-ad95-EXAMPLE0c374",
    "eventID": "7c6e3d04-0c3b-42f2-8589-EXAMPLE826c0",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "702f74c4-f692-4bfd-8491-EXAMPLEb1ac4",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```

Eventi Insights

CloudTrail Gli eventi Insights rilevano attività insolite relative alla frequenza delle chiamate API o al tasso di errore nel tuo AWS account analizzando l'attività di CloudTrail gestione. Gli eventi Insights forniscono informazioni importanti, come l'API associata, codice di errore, l'ora dell'incidente e le statistiche, che ti permettono di comprendere l'attività insolita e intervenire. A differenza di altri tipi di eventi acquisiti in un archivio dati di CloudTrail trail o event, gli eventi di Insights vengono registrati solo quando CloudTrail rilevano cambiamenti nell'utilizzo dell'API dell'account o nella registrazione del tasso di errore che differiscono significativamente dai modelli di utilizzo tipici dell'account. Per ulteriori informazioni, consulta Lavorare con CloudTrail Insights.

Alcuni esempi di attività che potrebbero generare eventi Insights:

- L'account in genere registra non più di 20 chiamate API `deleteBucket` Amazon S3 al minuto, ma l'account inizia a registrare una media di 100 chiamate API `deleteBucket` al minuto. Un evento Insights viene registrato all'inizio dell'attività insolita e un altro evento Insights viene registrato per contrassegnare la fine dell'attività insolita.
- Il tuo account registra in genere 20 chiamate al minuto verso l' `EC2AuthorizeSecurityGroupIngress`API Amazon, ma inizia a registrare zero chiamate verso`AuthorizeSecurityGroupIngress`. Un evento Insights viene registrato all'inizio dell'attività insolita; dieci minuti dopo, al termine dell'attività insolita, viene registrato un altro evento Insights per contrassegnare la fine dell'attività insolita.
- In genere, il tuo account registra meno di un errore `AccessDeniedException` in un periodo di sette giorni su API AWS Identity and Access Management , `DeleteInstanceProfile`. Il tuo account inizia a registrare una media di 12 errori `AccessDeniedException` al minuto nella chiamata API `DeleteInstanceProfile`. Un evento Insights viene registrato all'inizio dell'attività di tasso di errore insolita e un altro evento Insights viene registrato per contrassegnare la fine dell'attività insolita.

Questi esempi sono solo a scopo illustrativo. I risultati potrebbero variare a seconda del caso d'uso.

Per registrare gli eventi di CloudTrail Insights, devi abilitare esplicitamente gli eventi Insights su un trail o un data store di eventi nuovo o esistente. Per ulteriori informazioni sulla creazione di un trail, consulta Creazione di un percorso con la CloudTrail console. Per ulteriori informazioni sulla creazione di un datastore di eventi, consulta Crea un archivio dati sugli eventi per gli eventi Insights con la console.

Per gli eventi Insights vengono applicati costi aggiuntivi. Ti verrà addebitato separatamente se abiliti Insights sia per i percorsi che per i datastore di eventi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Sono stati registrati due eventi per mostrare attività insolite in CloudTrail Insights: un evento di inizio e un evento di fine. Nell'esempio seguente viene illustrato un singolo record di log di un evento Insights di inizio che si è verificato quando l'API `CompleteLifecycleAction` di Application Auto Scaling è stata chiamata un numero insolito di volte. Per gli eventi Insights, il valore di `eventCategory` è `Insight`. Un blocco `insightDetails` identifica lo stato dell'evento, l'origine, il nome, il tipo di Insights e il contesto, incluse le statistiche e le attribuzioni. Per ulteriori informazioni sul blocco `insightDetails`, consulta CloudTrail registra contenuti per gli eventi Insights per i percorsi.

```
{
```

```
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
```

```
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

Registrazione degli eventi di gestione

Per impostazione predefinita, i percorsi e i datastore di eventi registrano gli eventi di gestione e non includono gli eventi di dati o gli eventi Insights.

Per gli eventi di dati o Insights vengono applicati costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Indice

- Eventi di gestione
- Lettura e scrittura di eventi
- Registrazione degli eventi di gestione con AWS Management Console
  - Aggiornamento delle impostazioni degli eventi di gestione per un trail esistente
  - Aggiornamento delle impostazioni degli eventi di gestione per un archivio dati di eventi esistente
- Registrazione degli eventi di gestione con la AWS CLI

- Esempi: Registrazione di eventi di gestione per i percorsi
  - Esempi: registrazione degli eventi di gestione dei sentieri utilizzando selettori di eventi avanzati
  - Esempi: registrazione degli eventi di gestione dei trail utilizzando selettori di eventi di base
- Esempi: Registrazione degli eventi di gestione per i datastore di eventi
  - Esempio: escludi gli eventi AWS KMS di gestione
  - Esempio: escludi gli eventi di gestione di Amazon RDS
  - Esempio: escludi Servizio AWS eventi ed eventi dalle sessioni AWS Management Console
  - Esempio: escludi gli eventi di gestione per un'identità IAM specifica
- Registrazione degli eventi di gestione con la AWS SDKs

Eventi di gestione

Gli eventi di gestione forniscono visibilità sulle operazioni di gestione eseguite sulle risorse AWS dell'account. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Gli eventi di gestione di esempio includono:

- Configurazione della sicurezza (ad esempio, operazioni API IAM `AttachRolePolicy`)
- Registrazione di dispositivi (ad esempio, operazioni Amazon EC2 `CreateDefaultVpc` API)
- Configurazione delle regole per il routing dei dati (ad esempio, le operazioni delle EC2 `CreateSubnet` API Amazon)
- Configurazione della registrazione (ad esempio, AWS CloudTrail `CreateTrail` operazioni API)

Gli eventi di gestione possono includere anche eventi non API che si verificano nel tuo account. Ad esempio, quando un utente accede al tuo account, CloudTrail registra l'evento. `ConsoleLogin` Per ulteriori informazioni, consulta Eventi non API acquisiti da CloudTrail.

Per impostazione predefinita, i percorsi e i datastore di eventi vengono configurati per registrare gli eventi di gestione.

> **Note**
>
> La funzionalità di cronologia degli CloudTrail eventi supporta solo gli eventi di gestione. Non puoi escludere AWS KMS o escludere eventi Amazon RDS Data API dalla cronologia degli eventi; le impostazioni che applichi a un trail o a un event data store non si applicano

alla cronologia degli eventi. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Lettura e scrittura di eventi

Quando configuri il percorso o il datastore di eventi per la registrazione degli eventi di gestione, puoi specificare se desideri registrare gli eventi di sola lettura, gli eventi di sola scrittura o entrambi.

- Lettura

  Gli eventi di sola lettura includono le operazioni API che leggono le risorse, ma non le modificano. Ad esempio, gli eventi di sola lettura includono le operazioni Amazon EC2 `DescribeSecurityGroups` e `DescribeSubnets` API. Queste operazioni restituiscono solo informazioni sulle tue EC2 risorse Amazon e non modificano le configurazioni.
- Scrittura

  Gli eventi di tipo Write-only (sola scrittura) includono le operazioni API che modificano o possono modificare le risorse. Ad esempio, le operazioni Amazon EC2 `RunInstances` e `TerminateInstances` API modificano le tue istanze.

Esempio: registrazione degli eventi di lettura e scrittura per percorsi separati

L'esempio seguente mostra come è possibile configurare i trail in modo che le attività di log per un account vengano suddivise in bucket S3 separati: un bucket riceve gli eventi di sola lettura e un secondo bucket riceve eventi di sola scrittura.

1. Puoi creare un trail e scegliere un bucket S3 denominato `amzn-s3-demo-bucket1` per ricevere i file di log. Puoi quindi aggiornare il percorso e specificare che desideri registrare gli eventi Read (Lettura).
2. Puoi creare un secondo trail e scegliere un bucket S3 denominato `amzn-s3-demo-bucket2` per ricevere i file di log. Puoi quindi aggiornare il percorso per specificare che desideri registrare gli eventi Write (Scrittura).
3. Le operazioni Amazon EC2 `DescribeInstances` e `TerminateInstances` API avvengono nel tuo account.
4. L'operazione API `DescribeInstances` è un evento di sola lettura e corrisponde alle impostazioni del primo trail. Il percorso registra e consegna l'evento `aamzn-s3-demo-bucket1`.

5. L'operazione API `TerminateInstances` è un evento di sola scrittura e corrisponde alle impostazioni del secondo trail. Il percorso registra e consegna l'evento a. `amzn-s3-demo-bucket2`

Registrazione degli eventi di gestione con AWS Management Console

Questa sezione descrive come aggiornare le impostazioni degli eventi di gestione per un trail o un data store di eventi esistente.

Argomenti

- Aggiornamento delle impostazioni degli eventi di gestione per un trail esistente
- Aggiornamento delle impostazioni degli eventi di gestione per un archivio dati di eventi esistente

Aggiornamento delle impostazioni degli eventi di gestione per un trail esistente

Utilizzare la procedura seguente per aggiornare le impostazioni degli eventi di gestione per un trail esistente.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Apri la pagina Percorsi della CloudTrail console e scegli il nome del percorso.
3. Per Management events (Eventi di gestione), scegli Edit (Modifica).

   - Scegli se vuoi registrare gli eventi Read, Write o entrambi.
   - Scegli Escludi AWS KMS eventi per filtrare AWS Key Management Service (AWS KMS) gli eventi dal tuo Trail. L'impostazione predefinita prevede l'inclusione di tutti AWS KMS gli eventi.

     L'opzione per registrare o escludere AWS KMS gli eventi è disponibile solo se si registrano gli eventi di gestione sul percorso. Se si sceglie di non registrare gli eventi di gestione, AWS KMS gli eventi non vengono registrati e non è possibile modificare le impostazioni di registrazione AWS KMS degli eventi.

     AWS KMS azioni come `EncryptDecrypt`, e `GenerateDataKey` in genere generano un volume elevato (oltre il 99%) di eventi. Queste operazioni vengono ora registrate come eventi Read (Lettura). AWS KMS Le azioni pertinenti a basso volume come **`Disable`** e **`ScheduleKey`** (che in genere rappresentano meno dello 0,5% del volume degli AWS KMS eventi) vengono registrate come eventi di scrittura. **`Delete`**

Per escludere eventi ad alto volume come**`Encrypt`**, e **`DecryptGenerateDataKey`**, ma comunque registrare eventi pertinenti come e **`DisableScheduleKey`**, scegli di registrare gli eventi di gestione di Write **`Delete`** e deseleziona la casella di controllo Escludi eventi. AWS KMS

- Scegli Exclude Amazon RDS Data API events (Escludi eventi dell'API dati di Amazon RDS) per escludere dal percorso gli eventi dell'API dati di Amazon Relational Database Service. L'impostazione predefinita è includere tutti gli eventi dell'API dati di Amazon RDS. Per ulteriori informazioni sugli eventi dell'API dati di Amazon RDS, consulta Registrazione delle chiamate dell'API dati con AWS CloudTrail nella Guida per l'utente di Amazon RDS per Aurora.

4. Al termine, scegli Salva modifiche.

Aggiornamento delle impostazioni degli eventi di gestione per un archivio dati di eventi esistente

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Apri la pagina Event data store della CloudTrail console e scegli il nome del data store degli eventi.
3. Per gli eventi di gestione, scegli Modifica, quindi configura le seguenti impostazioni:
   a. Scegli tra Raccolta eventi semplice o Raccolta eventi avanzata:
      - Scegli Simple event collection se desideri registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere gli eventi AWS Key Management Service di gestione delle API di Amazon RDS Data.
      - Scegli Advanced event collection se desideri includere o escludere eventi di gestione in base ai valori dei campi avanzati di selezione degli eventi, inclusi i campi`eventName`, `eventTypeeventSource`, `euserIdentity.arn`.
   b. Se hai selezionato Raccolta di eventi semplice, scegli se registrare tutti gli eventi, registrare solo gli eventi di lettura o registrare solo gli eventi di scrittura. Puoi anche scegliere di escludere gli eventi AWS KMS di gestione di Amazon RDS.
   c. Se hai selezionato Raccolta eventi avanzata, effettua le seguenti selezioni:

i. In Log selector template, scegli un modello predefinito o Personalizzato per creare una configurazione personalizzata basata sui valori avanzati dei campi del selettore di eventi.

   Puoi scegliere tra i seguenti modelli predefiniti:

   - Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
   - Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
   - Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
   - Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
   - Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

ii. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio «Registra gli eventi di gestione delle sessioni». AWS Management Console Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

iii. Se hai scelto Personalizzato, in Advanced event selectors crea un'espressione basata sui valori avanzati dei campi del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

   A. Scegli tra i seguenti campi.

- **`readOnly`**— `readOnly` può essere impostato in modo che sia uguale a un valore di o. `true` `false` Quando è impostato su`false`, l'Event Data Store registra gli eventi di gestione di sola scrittura. Gli eventi di gestione di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi or. `Get*` `Describe*` Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia gli eventi di lettura che quelli di scrittura, non aggiungete un `readOnly` selettore.
- **`eventName`**— `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento di gestione, ad esempio `CreateAccessPoint` o`GetAccessPoint`.
- **`userIdentity.arn`**— Includi o escludi eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`sessionCredentialFromConsole`**— Includi o escludi eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- **`eventSource`**— È possibile utilizzarlo per includere o escludere fonti di eventi specifiche. In genere `eventSource` è una forma abbreviata del nome del servizio senza spazi plus`.amazonaws.com`. Ad esempio, puoi impostare `eventSource` equals to per registrare solo gli `ec2.amazonaws.com` eventi di EC2 gestione di Amazon.
- **`eventType`**— L'EventType da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale per escludere **`AwsServiceEvent`** gli eventi.Servizio AWS

B. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

Per informazioni su come CloudTrail valuta più condizioni, consulta. Come CloudTrail valuta più condizioni per un campo

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come

`eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

C. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

iv. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

d. Scegli Abilita l'acquisizione degli eventi di Insights per abilitare Insights. Per abilitare Insights, è necessario configurare un datastore di eventi di destinazione per raccogliere gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi.

Se scegli di abilitare Insights, procedi come segue.

i. Scegli l'archivio eventi di destinazione che registrerà gli eventi di Insights. Il datastore di eventi di destinazione raccoglierà gli eventi Insights in base all'attività degli eventi di gestione in questo datastore di eventi. Per informazioni su come creare il datastore di eventi di destinazione, consulta Creazione di un datastore di eventi di destinazione che registra gli eventi di Insights.

ii. Scegli i tipi di Insights. Puoi scegliere la frequenza delle chiamate API, la frequenza di errore API o entrambi. Devi abilitare la registrazione degli eventi di gestione Write (scrittura) per registrare gli eventi Insights per la frequenza di chiamate API. Devi abilitare la registrazione degli eventi di gestione Read o Write per registrare gli eventi Insights per la frequenza di errore API.

4. Al termine, scegli Salva modifiche.

Registrazione degli eventi di gestione con la AWS CLI

È possibile configurare i percorsi o i datastore di eventi per registrare gli eventi di gestione utilizzando la AWS CLI.

Argomenti

- Esempi: Registrazione di eventi di gestione per i percorsi
- Esempi: Registrazione degli eventi di gestione per i datastore di eventi

Esempi: Registrazione di eventi di gestione per i percorsi

Per verificare se il tuo trail sta registrando gli eventi di gestione, esegui il comando `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

L'esempio seguente restituisce le impostazioni di default per un trail. Per impostazione predefinita, i trail registrano tutti gli eventi di gestione, gli eventi di log da tutte le origini eventi e non registrano gli eventi di dati.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

È possibile utilizzare selettori di eventi di base o avanzati per registrare gli eventi di gestione. Non è possibile applicare sia selettori di eventi che selettori di eventi avanzati a un trail. Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti. Le sezioni seguenti forniscono esempi di come registrare gli eventi di gestione utilizzando selettori di eventi avanzati e selettori di eventi di base.

Argomenti

- Esempi: registrazione degli eventi di gestione dei sentieri utilizzando selettori di eventi avanzati
- Esempi: registrazione degli eventi di gestione dei trail utilizzando selettori di eventi di base

Esempi: registrazione degli eventi di gestione dei sentieri utilizzando selettori di eventi avanzati

L'esempio seguente crea un selettore di eventi avanzato per un percorso denominato *TrailName* per includere eventi di gestione di sola lettura e sola scrittura (omettendo il `readOnly` selettore), ma per escludere gli eventi (). AWS Key Management Service AWS KMS Poiché AWS KMS gli eventi vengono trattati come eventi gestionali e il loro volume può essere elevato, possono avere un impatto sostanziale sulla CloudTrail fattura se si dispone di più di un percorso che raccoglie gli eventi di gestione.

Se si sceglie di non registrare gli eventi di gestione, gli AWS KMS eventi non vengono registrati e non è possibile modificare le impostazioni di registrazione AWS KMS degli eventi.

Per ricominciare a registrare AWS KMS gli eventi in un percorso, rimuovete il `eventSource` selettore ed eseguite nuovamente il comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
```

```
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per avviare nuovamente la registrazione di eventi su un percorso, rimuovi il selettore `eventSource`, come mostrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

L'esempio successivo crea un selettore di eventi avanzato per un percorso denominato *`TrailName`* per includere eventi di gestione di sola lettura e sola scrittura (omettendo il `readOnly` selettore), ma per escludere gli eventi di gestione delle API di Amazon RDS Data. Per escludere gli eventi di gestione di Amazon RDS Data API, specifica l'origine dell'evento Amazon RDS Data API nel valore della stringa per il `eventSource` campo:. `rdsdata.amazonaws.com`

Se scegli di non registrare gli eventi di gestione, gli eventi di gestione di Amazon RDS Data API non vengono registrati e non puoi modificare le impostazioni di registrazione degli eventi di Amazon RDS Data API.

Per ricominciare a registrare gli eventi di gestione delle API di Amazon RDS Data su un trail, rimuovi il `eventSource` selettore ed esegui nuovamente il comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
```

```
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Per avviare nuovamente la registrazione di eventi su un percorso, rimuovi il selettore `eventSource`, come mostrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Esempi: registrazione degli eventi di gestione dei trail utilizzando selettori di eventi di base

Per configurare il trail per la registrazione di eventi di gestione, esegui il comando `put-event-selectors`. L'esempio seguente mostra come configurare il tuo trail per includere tutti gli eventi di

gestione per due oggetti S3. Puoi specificare da 1 a 5 selettori di eventi per un trail. Puoi specificare da 1 a 250 risorse di dati per un trail.

> **Note**
>
> Il numero massimo di risorse di dati S3 è 250, indipendentemente dal numero di selettori di eventi.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-demo-bucket/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"] }] }]'
```

L'esempio seguente restituisce il selettore di eventi configurato per il trail.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

Per escludere gli eventi AWS Key Management Service (AWS KMS) dai log di un percorso, esegui il `put-event-selectors` comando e aggiungi l'attributo `ExcludeManagementEventSources` con un valore di. `kms.amazonaws.com` L'esempio seguente crea un selettore di eventi per un percorso denominato in *`TrailName`* modo da includere eventi di gestione di sola lettura e sola scrittura, ma

escludendo gli eventi. AWS KMS Poiché AWS KMS può generare un volume elevato di eventi, l'utente in questo esempio potrebbe voler limitare gli eventi per gestire il costo di un trail.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

L'esempio restituisce il selettore di eventi configurato per il trail.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Per escludere gli eventi di gestione dell'API di Amazon RDS Data dai log di un percorso, esegui il `put-event-selectors` comando e aggiungi l'attributo `ExcludeManagementEventSources` con un valore di. `rdsdata.amazonaws.com` L'esempio seguente crea un selettore di eventi per un percorso denominato *`TrailName`* per includere eventi di gestione di sola lettura e sola scrittura, ma esclude gli eventi di gestione delle API di Amazon RDS Data. Poiché Amazon RDS Data API può generare un volume elevato di eventi di gestione, l'utente in questo esempio potrebbe voler limitare gli eventi per gestire il costo di un trail.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
```

```
        }
    ]
}
```

Per avviare nuovamente la registrazione AWS KMS o gli eventi di gestione delle API di Amazon RDS Data su un trail, passa una stringa vuota come valore di`ExcludeManagementEventSources`, come illustrato nel comando seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Per registrare AWS KMS gli eventi rilevanti in un percorso, ad esempio`Disable`, `Delete` con`ScheduleKey`, ma escludendo AWS KMS gli eventi ad alto volume come `EncryptDecrypt`, e`GenerateDataKey`, registra gli eventi di gestione di sola scrittura e mantieni l'impostazione predefinita per registrare AWS KMS gli eventi, come mostrato nell'esempio seguente.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Esempi: Registrazione degli eventi di gestione per i datastore di eventi

È possibile registrare gli eventi di gestione per gli archivi di dati di eventi configurando selettori di eventi avanzati.

I seguenti campi avanzati di selezione degli eventi sono supportati per la registrazione degli eventi di gestione negli archivi dati di eventi:

- **`eventCategory`**— È necessario impostare un `eventCategory` valore uguale `Management` agli eventi di gestione dei log. Questo è un campo obbligatorio.
- **`readOnly`**— `readOnly` può essere impostato su `Equals` un valore di `true` o`false`. Quando è impostato su`false`, l'Event Data Store registra gli eventi di gestione di sola scrittura. Gli eventi di gestione di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi or. `Get*` `Describe*` Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia gli eventi di lettura che quelli di scrittura, non aggiungete un `readOnly` selettore.

- **`eventName`**— `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento di gestione, ad esempio `CreateAccessPoint` o`GetAccessPoint`. È possibile utilizzare qualsiasi operatore con questo campo.
- **`userIdentity.arn`**— Includi o escludi eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`sessionCredentialFromConsole`**— Includi o escludi eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su Uguale o `NotEquals` con un valore di. `true`
- **`eventSource`**— È possibile utilizzarlo per includere o escludere fonti di eventi specifiche. In genere `eventSource` è una forma abbreviata del nome del servizio senza spazi plus`.amazonaws.com`. Ad esempio, puoi `eventSource` `Equals` impostare `ec2.amazonaws.com` la registrazione solo degli eventi di EC2 gestione di Amazon.
- **`eventType`**— L'EventType da includere o escludere. Ad esempio, è possibile impostare questo campo per `NotEquals` `AwsServiceEvent` escludere Servizio AWS gli eventi. È possibile utilizzare qualsiasi operatore con questo campo.

Per vedere se il datastore di eventi include eventi di gestione, esegui il comando get-event-data-store.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Di seguito è riportata una risposta di esempio. L'ora di creazione e dell'ultimo aggiornamento sono espressi nel formato `timestamp`.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

Per creare un datastore di eventi che includa tutti gli eventi di gestione, esegui il comando create-event-data-store. Non è necessario specificare i selettori di eventi avanzati per includere tutti gli eventi di gestione.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Esempi:

- Esempio: escludi gli eventi AWS KMS di gestione
- Esempio: escludi gli eventi di gestione di Amazon RDS
- Esempio: escludi Servizio AWS eventi ed eventi dalle sessioni AWS Management Console
- Esempio: escludi gli eventi di gestione per un'identità IAM specifica

Esempio: escludi gli eventi AWS KMS di gestione

Per creare un archivio dati di eventi che escluda gli eventi AWS Key Management Service (AWS KMS), esegui il `create-event-data-store` comando e specifica che `eventSource` non è ugualekms`.`amazonaws`.`com. L'esempio seguente crea un Event Data Store che include eventi di gestione di sola lettura e di sola scrittura, ma esclude gli eventi. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
```

```
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Esempio: escludi gli eventi di gestione di Amazon RDS

Per creare un event data store che escluda gli eventi di gestione di Amazon RDS Data API, esegui il `create-event-data-store` comando e specifica che `eventSource` non è uguale. `rdsdata.amazonaws.com` Nell'esempio seguente viene creato un datastore di eventi che include eventi di gestione di sola lettura e di sola scrittura, ma esclude gli eventi dell'API dati di Amazon RDS.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
```

```
        ]
    }
]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Esempio: escludi Servizio AWS eventi ed eventi dalle sessioni AWS Management Console

L'esempio seguente crea un archivio dati di eventi che registra gli eventi di gestione ma esclude gli Servizio AWS eventi e gli eventi provenienti dalle sessioni. AWS Management Console

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude Servizio AWS and console events",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventType","NotEquals": ["AwsServiceEvent"]},
            {"Field": "sessionCredentialFromConsole","NotEquals": ["true"]}
        ]
    }
]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Exclude Servizio AWS and console events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                },
                {
                    "Field": "sessionCredentialFromConsole",
                    "NotEquals": [
                        "true"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

Esempio: escludi gli eventi di gestione per un'identità IAM specifica

L'esempio seguente crea un archivio dati di eventi che registra gli eventi di gestione ma esclude gli eventi generati da. `bucket-scanner-role` `userIdentity`

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude events generated by bucket-scanner-role userIdentity",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "userIdentity.arn","NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

Di seguito è riportata una risposta di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Exclude events generated by bucket-scanner-role userIdentity",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
```

```
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

Registrazione degli eventi di gestione con la AWS SDKs

Usa l'GetEventSelectorsoperazione per vedere se il tuo trail sta registrando gli eventi di gestione per un trail. È possibile configurare i percorsi per registrare gli eventi di gestione con l'PutEventSelectorsoperazione. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS CloudTrail.

Esegui l'GetEventDataStoreoperazione per vedere se il tuo archivio dati degli eventi include eventi di gestione. È possibile configurare i data store degli eventi in modo da includere gli eventi di gestione eseguendo UpdateEventDataStorele operazioni CreateEventDataStoreor. Per ulteriori informazioni, consulta Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI e il Riferimento API di AWS CloudTrail.

Registrazione degli eventi di dati

Questa sezione descrive come registrare gli eventi relativi ai dati utilizzando la CloudTrail console e AWS CLI.

Per impostazione predefinita, i percorsi e i datastore di eventi non registrano gli eventi di dati. Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Gli eventi di dati forniscono informazioni sulle operazioni eseguite in una risorsa o al suo interno. Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati.

Gli eventi di dati di esempio includono:

- Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject``DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket S3.
- AWS Lambda attività di esecuzione della funzione (l'API). `Invoke`
- CloudTrail `PutAuditEvents`attività su un canale CloudTrail Lake che viene utilizzata per registrare eventi dall'esterno AWS.
- Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.

Puoi utilizzare selettori di eventi avanzati per creare selettori dettagliati, che ti aiutano a controllare i costi registrando solo gli eventi specifici di interesse per i tuoi casi d'uso. Ad esempio, puoi utilizzare selettori di eventi avanzati per registrare chiamate API specifiche aggiungendo un filtro sul campo. `eventName` Per ulteriori informazioni, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.

> **Note**
>
> Gli eventi registrati dai tuoi percorsi sono disponibili su Amazon EventBridge. Ad esempio, se decidi di registrare gli eventi di dati per gli oggetti S3 ma non gli eventi di gestione, il percorso elabora e registra solo gli eventi di dati per gli oggetti S3 specificati. Gli eventi relativi ai dati per questi oggetti S3 sono disponibili in Amazon EventBridge. Per ulteriori informazioni, consulta gli eventi di AWS servizio forniti CloudTrail nella Amazon EventBridge User Guide e nell'AWS Events Reference.

Indice

- Eventi di dati
  - Eventi di dati supportati da AWS CloudTrail
  - Esempi: registrazione di eventi di dati per oggetti Amazon S3
  - Registrazione degli eventi relativi ai dati per gli oggetti S3 in altri account AWS
- Eventi di sola lettura e di sola scrittura

- Registrazione degli eventi relativi ai dati con il AWS Management Console
- Registrazione degli eventi relativi ai dati con AWS Command Line Interface
  - Registrazione degli eventi relativi ai dati per i sentieri con il AWS CLI
    - Registra gli eventi relativi ai dati per i percorsi utilizzando selettori di eventi avanzati
    - Registra tutti gli eventi Amazon S3 per un bucket Amazon S3 utilizzando selettori di eventi avanzati
    - Registrazione di eventi Amazon S3 su AWS Outposts utilizzando i selettori di eventi avanzati
    - Registrazione di eventi utilizzando i selettori di eventi di base
  - Registrazione degli eventi relativi ai dati per gli archivi dati degli eventi con AWS CLI
    - Includi tutti gli eventi Amazon S3 per un bucket specifico
    - Inclusione di Amazon S3 negli eventi AWS Outposts
- Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati
  - Come CloudTrail valuta più condizioni per un campo
    - Esempio che mostra più condizioni per il campo resources.ARN
  - AWS CLI esempi per filtrare gli eventi relativi ai dati
    - Esempio 1: filtraggio sul campo eventName
    - Esempio 2: filtraggio in base ai campi resources.ARN e userIdentity.arn
    - Esempio 3: filtraggio sui eventName campi resources.type and per escludere singoli oggetti eliminati da un evento Amazon DeleteObjects S3
- Registrazione di eventi di dati per la conformità di AWS Config
- Registrazione degli eventi relativi ai dati con AWS SDKs

Eventi di dati

La tabella seguente mostra i tipi di risorse disponibili per i percorsi e gli archivi di dati di eventi. La colonna Tipo di risorsa (console) mostra la selezione appropriata nella console. La colonna del valore resources.type mostra il `resources.type` valore da specificare per includere eventi di dati di quel tipo nel tuo trail o event data store utilizzando o. AWS CLI CloudTrail APIs

Per i trail, puoi utilizzare selettori di eventi di base o avanzati per registrare gli eventi di dati per oggetti Amazon S3 in bucket generici, funzioni Lambda e tabelle DynamoDB (mostrate nelle prime tre righe della tabella). Puoi utilizzare solo selettori di eventi avanzati per registrare i tipi di risorse mostrati nelle righe rimanenti.

Per i datastore di eventi, per includere gli eventi di dati è possibile utilizzare solo i selettori di eventi avanzati.

Eventi di dati supportati da AWS CloudTrail

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS Backup	AWS Backup Attività dell'API Search Data sulle offerte di lavoro di ricerca.	AWS Backup Dati di ricerca APIs	`AWS::Backup::SearchJob`
AWS IoT	AWS IoT Attività delle API sui certificati.	Certificato IoT	`AWS::IoT::Certificate`
AWS IoT	AWS IoT Attività delle API sugli oggetti.	Cosa IoT	`AWS::IoT::Thing`
AWS Private CA	AWS Private CA Connettore per l'attività dell'API di Active Directory.	AWS Private CA Connettore per Active Directory	`AWS::PCAConnectorAD::Connector`
AWS Private CA	AWS Private CA Connettore per l'attività dell'API SCEP.	AWS Private CA Connettore per SCEP	`AWS::PCAConnectorSCEP::Connector`
Amazon RDS	Attività dell'API Amazon RDS su un cluster DB.	API dati RDS - Cluster DB	`AWS::RDS::DBCluster`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject` , e operazion	S3	`AWS::S3::Object`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
	i `PutObject` API) su oggetti in bucket generici.		
Amazon S3	Attività dell'API Amazon S3 sui punti di accesso.	Punto di accesso S3	`AWS::S3::AccessPoint`
Amazon S3	Attività delle API a livello di oggetto di Amazon S3 (ad esempio `GetObject` `DeleteObject`, e operazioni `PutObject` API) sugli oggetti nei bucket di directory.	S3 Express	`AWS::S3Express::Object`
Amazon S3	Attività delle API dei punti di accesso Amazon S3 Object Lambda, ad esempio chiamate a e. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3	Attività FSx delle API Amazon sui volumi.	FSx Volume	`AWS::FSx::Volume`
Tabelle di Amazon S3	Attività dell'API Amazon S3 sulle tabelle.	Tabella S3	`AWS::S3Tables::Table`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Tabelle di Amazon S3	Attività dell'API Amazon S3 su bucket da tabella.	Secchio da tavolo S3	`AWS::S3Tables::TableBucket`
Amazon S3 su Outposts	Attività dell'API a livello di oggetto di Amazon S3 su Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SNS	Operazioni dell'API `Publish` Amazon SNS sugli endpoint della piattaforma.	Endpoint della piattaforma SNS	`AWS::SNS::PlatformEndpoint`
Amazon SNS	Operazioni API `Publish` e `PublishBatch` di Amazon SNS sugli argomenti.	Argomento SNS	`AWS::SNS::Topic`
Amazon SQS	Attività dell'API Amazon SQS sui messaggi.	SQS	`AWS::SQS::Queue`
Catena di approvvigionamento di AWS	Catena di approvvigionamento di AWS Attività dell'API su un'istanza.	Catena di fornitura	`AWS::SCN::Instance`
Amazon SWF	Attività dell'API Amazon SWF sui domini.	Dominio SWF	`AWS::SWF::Domain`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS AppConfig	AWS AppConfig Attività dell'API per operazioni di configurazione come chiamate a `StartConfiguration` `Session` e `GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS AppSync	AWS AppSync Attività delle API su AppSync GraphQL APIs.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`
Amazon Aurora DSQL	Attività dell'API SQL di Amazon Aurora sulle risorse del cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
AWS Scambio di dati B2B	Attività dell'API Scambio di dati B2B per operazioni Transformer, come le chiamate a `GetTransformerJob` e `StartTransformerJob` .	Scambio di dati B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Attività dell'API Amazon Bedrock sull'alias di un agente.	Alias dell'agente Bedrock	`AWS::Bedrock::AgentAlias`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle chiamate asincrone.	Richiamo asincrono Bedrock	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	Attività dell'API Amazon Bedrock su un alias di flusso.	Alias di flusso Bedrock	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui guardrail.	Parapetto Bedrock	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Attività dell'API Amazon Bedrock sugli agenti in linea.	Agente in linea Bedrock Invoke	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una knowledge base.	Knowledge base Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui modelli.	Modello Bedrock	`AWS::Bedrock::Model`
Amazon Bedrock	Attività dell'API Amazon Bedrock sui prompt.	Richiesta Bedrock	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	Attività dell'API Amazon Bedrock nelle sessioni.	Sessione Bedrock	`AWS::Bedrock::Session`
Amazon Bedrock	Attività dell'API Amazon Bedrock sulle esecuzioni dei flussi.	Esecuzione del flusso di base	`AWS::Bedrock::FlowExecution`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Bedrock	Attività dell'API Amazon Bedrock su una politica di ragionamento automatico.	Politica di ragionamento automatizzato di base	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Attività dell'API Amazon Bedrock su una versione di policy di ragionamento automatico.	Versione della politica di ragionamento automatico Bedrock	`AWS::Bedrock::AutomatedReasoningPolicyVersion`
AWS Cloud Map	AWS Cloud Map Attività dell'API su un namespace.	AWS Cloud Map spazio dei nomi	`AWS::ServiceDiscovery::Namespace`
AWS Cloud Map	AWS Cloud Map Attività dell'API su un servizio.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
Amazon CloudFront	CloudFront Attività delle API su un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS CloudTrail	CloudTrail `PutAuditEvents` attività su un canale CloudTrail Lake che viene utilizzato per registrare eventi dall'esterno AWS.	CloudTrail canale	`AWS::CloudTrail::Channel`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon CloudWatch	Attività dell' CloudWatch API Amazon sulle metriche.	CloudWatch parametro	`AWS::CloudWatch::Metric`
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sui monitor.	Monitor di Network Flow Monitor	`AWS::NetworkFlowMonitor::Monitor`
Monitoraggio del flusso di CloudWatch rete Amazon	Attività dell'API Amazon CloudWatch Network Flow Monitor sugli ambiti.	Ambito di Network Flow Monitor	`AWS::NetworkFlowMonitor::Scope`
Amazon CloudWatch RUM	Attività dell'API Amazon CloudWatch RUM sui monitor delle app.	Monitoraggio delle app RUM	`AWS::RUM::AppMonitor`
Amazon CodeGuru Profiler	CodeGuru Attività dell'API Profiler sui gruppi di profilazione.	CodeGuru Gruppo di profilazione Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su una personalizzazione.	CodeWhisperer personalizzazione	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Attività dell' CodeWhisperer API Amazon su un profilo.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Cognito	Attività dell'API Amazon Cognito sui pool di identità di Amazon Cognito.	Pool di identità di Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Data Exchange Attività delle API sugli asset.	Risorsa Data Exchange	`AWS::DataExchange::Asset`
AWS Deadline Cloud	Deadline CloudAttività delle API sulle flotte.	Deadline Cloud flotta	`AWS::Deadline::Fleet`
AWS Deadline Cloud	Deadline Cloudattività delle API sui lavori.	Deadline Cloud lavoro	`AWS::Deadline::Job`
AWS Deadline Cloud	Deadline Cloudattività delle API in coda.	Deadline Cloud coda	`AWS::Deadline::Queue`
AWS Deadline Cloud	Deadline CloudAttività delle API sui lavoratori.	Deadline Cloud lavoratore	`AWS::Deadline::Worker`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon DynamoDB	Attività delle API a livello di elemento di Amazon DynamoDB sulle tabelle (ad esempio `PutItem`, `DeleteItem` e operazioni API). `UpdateItem` **Note** Per le tabelle con flussi abilitati, il campo `resources` nell'evento di dati contiene sia `AWS::DynamoDB::Stream` che `AWS::DynamoDB::Table`. Se specifichi `AWS::DynamoDB::Table` come `resources.type`, per impostazione predefini	DynamoDB	`AWS::DynamoDB::Table`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
	ta verranno registrati sia gli eventi della tabella DynamoDB che quelli dei flussi DynamoDB. Per escludere gli eventi di streaming, aggiungi un filtro sul campo. `eventName`		
Amazon DynamoDB	Attività dell'API Amazon DynamoDB sui flussi	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct APIs, ad esempio `GetSnapshotBlock` e su `PutSnapshotBlock` istantanee e `ListChangedBlocks` Amazon EBS.	Amazon EBS diretto APIs	`AWS::EC2::Snapshot`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Elastic Kubernetes Service	Attività dell'API Amazon Elastic Kubernetes Service sulle dashboard.	Pannello di controllo di Amazon Elastic Kubernetes Service	`AWS::EKS::Dashboard`
Amazon EMR	Attività dell'API Amazon EMR su un'area di lavoro di log write-ahead.	Workspace di registrazione write-ahead EMR	`AWS::EMRWAL::Workspace`
AWS SMS di messaggistica per l'utente finale	AWS Attività dell'API SMS di messaggistica per l'utente finale sulle identità di origine.	Identità di origine tramite SMS Voice	`AWS::SMSVoice::OriginationIdentity`
AWS SMS di messaggistica per l'utente finale	AWS Attività dell'API SMS di messaggistica per l'utente finale sui messaggi.	Messaggio vocale SMS	`AWS::SMSVoice::Message`
AWS Messaggistica sociale per utenti finali	AWS Attività dell'API Social Messaging per l'utente finale sul numero di telefono IDs.	ID del numero di telefono di messaggistica sociale	`AWS::SocialMessaging::PhoneNumberId`
AWS Social di messaggistica per utenti finali	AWS Attività dell'API End User Messaging Social su Waba IDs.	ID Waba per la messaggistica sociale	`AWS::SocialMessaging::WabaId`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon FinSpace	Attività dell'API Amazon FinSpace sugli ambienti	FinSpace	`AWS::FinSpace::Environment`
Amazon GameLift Stream	L'attività delle API di streaming di Amazon GameLift Streams sulle applicazioni.	GameLift Applicazione Streams	`AWS::GameLiftStreams::Application`
Amazon GameLift Stream	Attività delle API di streaming di Amazon GameLift Streams sui gruppi di stream.	GameLift Gruppo di stream Streams	`AWS::GameLiftStreams::StreamGroup`
AWS Glue	AWS Glue Attività dell'API su tabelle create da Lake Formation.	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	Attività dell' GuardDuty API Amazon per un rilevatore.	GuardDuty rilevatore	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging attività delle API sugli archivi dati.	MedicalImaging archivio dati	`AWS::MedicalImaging::Datastore`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass su una versione componente. **Note** Greengrass non registra gli eventi di accesso negato.	Versione componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
AWS IoT Greengrass Version 2	Attività dell'API Greengrass da un dispositivo principale Greengrass in una distribuzione. **Note** Greengrass non registra gli eventi di accesso negato.	Implementazione IoT Greengrass	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Attività dell' SiteWise API IoT sugli asset.	SiteWise Risorse IoT	`AWS::IoTSiteWise::Asset`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
AWS IoT SiteWise	Attività dell' SiteWise API IoT su serie temporali.	Serie SiteWise temporali IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT SiteWise Assistente	Attività dell'API Sitewise Assistant sulle conversazioni.	Conversazione con Sitewise Assistant	`AWS::SitewiseAssistant::Conversation`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'entità.	TwinMaker Entità IoT	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Attività dell' TwinMaker API IoT su un'area di lavoro.	Spazio di TwinMaker lavoro IoT	`AWS::IoTTwinMaker::Workspace`
Classificazione intelligente di Amazon Kendra	Attività dell'API Amazon Kendra Intelligent Ranking sui piani di esecuzione di rescore.	Classificazione Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces su una tabella.	Tabella Cassandra	`AWS::Cassandra::Table`
Amazon Keyspaces (per Apache Cassandra)	Attività dell'API Amazon Keyspaces (per Apache Cassandra) sugli stream Cassandra CDC.	Stream Cassandra CDC	`AWS::Cassandra::Stream`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sugli stream.	Stream Kinesis	`AWS::Kinesis::Stream`
Flusso di dati Amazon Kinesis	Attività dell'API Kinesis Data Streams sui consumatori di streaming.	Kinesis Stream Consumer	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Attività dell'API Kinesis Video Streams sui flussi video, ad esempio chiamate verso e. `GetMedia` `PutMedia`	Flusso video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Lambda attività di esecuzione delle funzioni (l'API). `Invoke`	Lambda	`AWS::Lambda::Function`
Amazon Location Maps	Attività dell'API Amazon Location Maps.	Mappe geografiche	`AWS::GeoMaps::Provider`
Luoghi di Amazon Location	Attività dell'API Amazon Location Places.	Luoghi geografici	`AWS::GeoPlaces::Provider`
Route di Amazon Location	Attività dell'API Amazon Location Routes.	Percorsi geografici	`AWS::GeoRoutes::Provider`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Machine Learning	Attività dell'API di Machine Learning sui modelli ML.	Apprendimento automatico MlModel	`AWS::MachineLearning::MlModel`
Blockchain gestita da Amazon	Attività dell'API Blockchain gestita da Amazon su una rete.	Rete Blockchain gestita	`AWS::ManagedBlockchain::Network`
Blockchain gestita da Amazon	Chiamate JSON-RPC di Blockchain gestita da Amazon sui nodi Ethereum, come `eth_getBalance` o `eth_getBlockByNumber` .	Blockchain gestita	`AWS::ManagedBlockchain::Node`
Query su Blockchain gestita da Amazon	Attività dell'API Amazon Managed Blockchain Query.	Query Blockchain gestita	`AWS::ManagedBlockchainQuery::QueryAPI`
Amazon Managed Workflows for Apache Airflow	Attività dell'API Amazon MWAA negli ambienti.	Apache Airflow gestito	`AWS::MWAA::Environment`
Grafo Amazon Neptune	Attività dell'API dati, ad esempio query, algoritmi o ricerca vettoriale, su un grafo Neptune.	Grafo Neptune	`AWS::NeptuneGraph::Graph`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon One Enterprise	Attività dell'API Amazon One Enterprise su un UKey.	Amazon Uno UKey	`AWS::One::UKey`
Amazon One Enterprise	Attività dell'API Amazon One Enterprise sugli utenti.	Utente Amazon One	`AWS::One::User`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sugli alias.	Alias di crittografia dei pagamenti	`AWS::PaymentCryptography::Alias`
AWS Payment Cryptography	AWS Payment Cryptography Attività delle API sulle chiavi.	Chiave di crittografia dei pagamenti	`AWS::PaymentCryptography::Key`
Amazon Pinpoint	Attività dell'API Amazon Pinpoint su applicazioni di targeting per dispositivi mobili.	Applicazione di targeting mobile	`AWS::Pinpoint::App`
App Amazon Q	Attività delle API di dati su Amazon Q Apps.	App Amazon Q	`AWS::QApps::QApp`
App Amazon Q	Attività delle API di dati nelle sessioni di Amazon Q App.	Sessione dell'app Amazon Q	`AWS::QApps::QAppSession`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Q Business	Attività dell'API Amazon Q Business su un'applicazione.	Applicazione Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Business	Attività dell'API Amazon Q Business su un'origine dati.	Origine dati Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Business	Attività dell'API Amazon Q Business su un indice.	Indice Amazon Q Business	`AWS::QBusiness::Index`
Amazon Q Business	Attività dell'API Amazon Q Business su un'esperienza Web.	Esperienza Web Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Attività dell'API Amazon Q Developer su un'integrazione.	Integrazione con Q Developer	`AWS::QDeveloper::Integration`
Amazon Q Developer	Attività dell'API Amazon Q Developer sulle indagini operative.	AIOps Gruppo di indagine	`AWS::AIOps::InvestigationGroup`
Amazon SageMaker AI	`InvokeEndpointWithResponseStream` Attività di Amazon SageMaker AI sugli endpoint.	SageMaker Endpoint AI	`AWS::SageMaker::Endpoint`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui feature store.	SageMaker AI feature store	`AWS::SageMaker::FeatureGroup`
Amazon SageMaker AI	Attività dell'API Amazon SageMaker AI sui componenti di prova sperimentali.	SageMaker Component e di prova dell'esperimento AI Metrics	`AWS::SageMaker::ExperimentTrialComponent`
AWS Signer	Attività dell'API Signer sulla firma dei lavori.	Firmatario che firma un lavoro	`AWS::Signer::SigningJob`
AWS Signer	Attività dell'API Signer sulla firma dei profili.	Profilo di firma del firmatario	`AWS::Signer::SigningProfile`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui set di configurazione.	Set di configurazione SES	`AWS::SES::ConfigurationSet`
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sulle identità e-mail.	Identità SES	`AWS::SES::EmailIdentity`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Simple Email Service	Attività dell'API Amazon Simple Email Service (Amazon SES) sui modelli.	Modello SES	`AWS::SES::Template`
Amazon SimpleDB	Attività dell'API Amazon SimpleDB sui domini.	Dominio SimpleDB	`AWS::SDB::Domain`
AWS Step Functions	Attività dell'API Step Functions sulle attività.	Step Functions	`AWS::StepFunctions::Activity`
AWS Step Functions	Attività dell'API Step Functions su macchine a stati.	Macchina a stati di Step Functions	`AWS::StepFunctions::StateMachine`
AWS Systems Manager	Attività dell'API Systems Manager sui canali di controllo.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Systems Manager	Attività dell'API Systems Manager sulle valutazioni dell'impatto.	Valutazione dell'impatto SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Attività dell'API Systems Manager sui nodi gestiti.	Nodo gestito da Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sui database.	Database Timestream	`AWS::Timestream::Database`

Servizio AWS	Descrizione	Tipo di risorsa (console)	valore resources.type
Amazon Timestream	Attività dell'API Amazon Timestream sugli endpoint regionali.	Endpoint regionale Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Attività dell'API `Query` di Amazon Timestream sulle tabelle.	Tabella Timestream	`AWS::Timestream::Table`
Autorizzazioni verificate da Amazon	Attività dell'API Autorizzazioni verificate da Amazon su un archivio di policy.	Autorizzazioni verificate da Amazon	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client su un dispositivo.	Dispositivo Thin client	`AWS::ThinClient::Device`
Amazon WorkSpaces Thin Client	WorkSpaces Attività dell'API Thin Client in un ambiente.	Ambiente Thin client	`AWS::ThinClient::Environment`
AWS X-Ray	Attività dell'API X-Ray sulle tracce.	Traccia a raggi X	`AWS::XRay::Trace`

Per registrare gli eventi CloudTrail relativi ai dati, è necessario aggiungere in modo esplicito ogni tipo di risorsa per cui si desidera raccogliere attività. Per ulteriori informazioni, consultare Creazione di un percorso con la CloudTrail console e Crea un archivio dati di CloudTrail eventi per gli eventi con la console.

In un percorso o un datastore di eventi a singola Regione, puoi registrare gli eventi di dati solo per le risorse a cui è possibile accedere in tale Regione. Sebbene i bucket S3 siano globali, le AWS Lambda funzioni e le tabelle DynamoDB sono regionali.

Per la registrazione degli eventi di dati sono previsti costi aggiuntivi. Per i CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

Esempi: registrazione di eventi di dati per oggetti Amazon S3

Registrazione di eventi di dati per tutti gli oggetti S3 in un bucket S3

L'esempio seguente mostra il funzionamento della registrazione quando si configura la registrazione di tutti gli eventi di dati per un bucket S3 denominato `amzn-s3-demo-bucket`. In questo esempio, l' CloudTrail utente ha specificato un prefisso vuoto e l'opzione per registrare sia gli eventi di lettura che quelli di scrittura dei dati.

1. Un utente carica un oggetto in `amzn-s3-demo-bucket`.
2. L'operazione API `PutObject` è un'API a livello di oggetti di Amazon S3. Viene registrato come evento di dati in CloudTrail. Poiché l' CloudTrail utente ha specificato un bucket S3 con un prefisso vuoto, gli eventi che si verificano su qualsiasi oggetto in quel bucket vengono registrati. Il percorso o il datastore di eventi elabora e registra l'evento.
3. Un altro utente carica un oggetto in `amzn-s3-demo-bucket2`.
4. L'operazione API `PutObject` si è verificata in un oggetto in un bucket S3 che non è stato specificato per il percorso o il datastore di eventi. Il percorso o il datastore di eventi non registra l'evento.

Registrazione di eventi di dati per oggetti S3 specifici

L'esempio seguente mostra il funzionamento della registrazione quando si configura un percorso o un datastore di eventi per la registrazione degli eventi per oggetti S3 specifici. In questo esempio, l' CloudTrail utente ha specificato un bucket S3 denominato**`amzn-s3-demo-bucket3`**, con il prefisso e l'opzione per registrare solo gli eventi di ***`my-images`*** scrittura dei dati.

1. Un utente elimina un oggetto che inizia con il prefisso `my-images` nel bucket, ad esempio `arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`.
2. L'operazione API `DeleteObject` è un'API a livello di oggetti di Amazon S3. Viene registrato come evento Write data in. CloudTrail L'evento si è verificato su un oggetto corrispondente al bucket S3 e al prefisso specificati nel percorso o nel datastore di eventi. Il percorso o il datastore di eventi elabora e registra l'evento.
3. Un altro utente elimina un oggetto che inizia con un prefisso diverso nel bucket S3, ad esempio `arn:aws:s3:::amzn-s3-demo-bucket3/my-videos/example.avi`.

4. L'evento si è verificato su un oggetto che non corrisponde al prefisso specificato nel percorso o nel datastore di eventi. Il percorso o il datastore di eventi non registra l'evento.
5. Un utente chiama l'operazione API `GetObject` per l'oggetto `arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`.
6. L'evento si è verificato su un bucket e sul prefisso specificati nel percorso o nel datastore di eventi, ma `GetObject` è un'API a livello di oggetto Amazon S3 di tipo di sola lettura. Viene registrato come evento Read data in CloudTrail e il trail o event data store non è configurato per registrare gli eventi di lettura. Il percorso o il datastore di eventi non registra l'evento.

> **Note**
>
> Per i percorsi, in caso di registrazione di eventi di dati per bucket Amazon S3 specifici, è consigliabile non utilizzare un bucket Amazon S3 per il quale è attiva la registrazione degli eventi di dati per la ricezione dei file di log specificati nella sezione relativa agli eventi di dati. L'utilizzo dello stesso bucket Amazon S3 fa sì che il percorso registri un evento di dati ogni volta che i file di log vengono distribuiti nel bucket Amazon S3. I fil di log sono eventi aggregati distribuiti a intervalli (non in un rapporto uno a uno). L'evento viene registrato nel successivo file di log. Ad esempio, quando CloudTrail consegna i log, l'`PutObject`evento si verifica nel bucket S3. Se il bucket S3 viene specificato anche nella sezione degli eventi di dati, il trail elabora e registra l'evento `PutObject` come un evento di dati. Questa azione è un altro evento `PutObject` e il trail elabora e registra di nuovo l'evento.
> Per evitare di registrare gli eventi relativi ai dati per il bucket Amazon S3 in cui ricevi i file di log, se configuri un trail per registrare tutti gli eventi relativi ai dati di Amazon S3 nel AWS tuo account, prendi in considerazione la possibilità di configurare la consegna dei file di log a un bucket Amazon S3 che appartiene a un altro account. AWS Per ulteriori informazioni, consulta Ricezione di file di CloudTrail registro da più account.

Registrazione degli eventi relativi ai dati per gli oggetti S3 in altri account AWS

Quando configuri il tuo trail per registrare gli eventi relativi ai dati, puoi anche specificare oggetti S3 che appartengono ad altri account. AWS Quando si verifica un evento in un oggetto specifico, CloudTrail valuta se l'evento corrisponde a qualsiasi trail in ciascun account. Se l'evento corrisponde alle impostazioni di un trail, il trail elabora e registra l'evento per tale account. In genere, sia gli intermediari API che i proprietari di risorse possono ricevere eventi.

Se disponi di un oggetto S3 e lo specifichi nel trail, il trail registra gli eventi che si verificano nell'oggetto nel tuo account. Poiché sei il proprietario dell'oggetto, il trail registra anche gli eventi quando altri account chiamano l'oggetto.

Se specifichi un oggetto S3 nel trail e un altro account è proprietario dell'oggetto, il trail registra solo gli eventi che si verificano in tale oggetto nel tuo account. Il trail non registra gli eventi che si verificano in altri account.

Esempio: registrazione di eventi di dati per un oggetto Amazon S3 per due account AWS

L'esempio seguente mostra come due AWS account si configurano CloudTrail per registrare gli eventi per lo stesso oggetto S3.

1. Nel tuo account vuoi che il trail registri gli eventi di dati per tutti gli oggetti nel bucket S3 denominato `amzn-s3-demo-bucket`. Puoi configurare le tracce specificando il bucket S3 con un prefisso di oggetto vuoto.
2. Bob dispone di un account distinto che dispone dell'accesso al bucket S3. Bob vuole inoltre registrare gli eventi di dati per tutti gli oggetti nello stesso bucket S3. Durante la configurazione del suo trail specifica lo stesso bucket S3 con un prefisso di oggetto vuoto.
3. Bob carica un oggetto nel bucket S3 con l'operazione API `PutObject`.
4. Questo evento si verifica nel suo account e corrisponde alle impostazioni del suo trail. Il trail di Bob elabora e registra l'evento.
5. Poiché sei il proprietario del bucket S3 e l'evento corrisponde alle impostazioni del tuo trail, anche il tuo trail elabora e registra lo stesso evento. Poiché ora ci sono due copie dell'evento (una registrata nel percorso di Bob e una nella tua), vengono CloudTrail addebitate due copie dell'evento relativo ai dati.
6. Carichi un oggetto nel bucket S3.
7. Questo evento si verifica nel tuo account e corrisponde alle impostazioni del tuo trail. Il tuo trail elabora e registra l'evento.
8. Poiché l'evento non si è verificato nell'account di Bob e lui non possiede il bucket S3, il percorso di Bob non registra l'evento. CloudTrail addebita solo una copia di questo evento relativo ai dati.

Esempio: registrazione degli eventi relativi ai dati per tutti i bucket, incluso un bucket S3 utilizzato da due account AWS

L'esempio seguente mostra il comportamento di registrazione quando l'opzione Seleziona tutti i bucket S3 del tuo account è abilitata per i trail che raccolgono gli eventi relativi ai dati in un account. AWS

1. Nel tuo account, desideri che il tuo trail registri gli eventi di dati per tutti i bucket S3. Puoi configurare il percorso scegliendo gli eventi Read (Lettura), Write (Scrittura) o entrambi per All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) in Data events (Eventi di dati).
2. Bob ha un account separato a cui è stato concesso l'accesso a un bucket S3 nel tuo account. Vuole registrare gli eventi di dati per il bucket a cui ha accesso. Egli configura il suo trail per ottenere gli eventi di dati per tutti i bucket S3.
3. Bob carica un oggetto nel bucket S3 con l'operazione API `PutObject`.
4. Questo evento si verifica nel suo account e corrisponde alle impostazioni del suo trail. Il trail di Bob elabora e registra l'evento.
5. Poiché sei il proprietario del bucket S3 e l'evento corrisponde alle impostazioni del tuo trail, anche il tuo trail elabora e registra l'evento. Poiché ora ci sono due copie dell'evento (una registrata nel percorso di Bob e l'altra nel tuo), CloudTrail addebita a ciascun account una copia dell'evento relativo ai dati.
6. Carichi un oggetto nel bucket S3.
7. Questo evento si verifica nel tuo account e corrisponde alle impostazioni del tuo trail. Il tuo trail elabora e registra l'evento.
8. Poiché l'evento non si è verificato nell'account di Bob e lui non possiede il bucket S3, il percorso di Bob non registra l'evento. CloudTrail addebita solo una copia di questo evento relativo ai dati nel tuo account.
9. Un terzo utente, Mary, ha accesso al bucket S3 ed esegue un'operazione `GetObject` sul bucket. Ella ha un trail configurato per registrare gli eventi di dati su tutti i bucket S3 nel suo account. Poiché è la chiamante dell'API, CloudTrail registra un evento relativo ai dati nelle sue tracce. Anche se Bob ha accesso al bucket, non è il proprietario della risorsa, quindi questa volta nel suo trail non viene registrato alcun evento. Come proprietario delle risorse, ricevi un evento nel tuo trail riguardo all'operazione `GetObject` che Mary ha richiamato. CloudTrail esegue un addebito sul tuo account e su quello di Mary di ogni copia dell'evento di dati: una nel trail di Mary e una nel tuo.

Eventi di sola lettura e di sola scrittura

Quando configuri il percorso o il datastore di eventi per la registrazione degli eventi di dati e di gestione, puoi specificare se desideri registrare gli eventi di sola lettura, gli eventi di sola scrittura o entrambi.

- Lettura

  Gli eventi Read (Lettura) includono le operazioni API che leggono le risorse, ma non le modificano. Ad esempio, gli eventi di sola lettura includono le operazioni Amazon EC2 `DescribeSecurityGroups` e `DescribeSubnets` API. Queste operazioni restituiscono solo informazioni sulle tue EC2 risorse Amazon e non modificano le configurazioni.
- Scrittura

  Gli eventi Write (Scrittura) includono le operazioni API che modificano o potrebbero modificare le risorse. Ad esempio, le operazioni Amazon EC2 `RunInstances` e `TerminateInstances` API modificano le tue istanze.

Esempio: registrazione degli eventi di lettura e scrittura per percorsi separati

L'esempio seguente mostra come configurare i trail per suddividere l'attività di registro di un account in bucket S3 separati: un bucket denominato amzn-s3-demo-bucket1 riceve eventi di sola lettura e un secondo amzn-s3-demo-bucket2 riceve eventi di sola scrittura.

1. Si crea un trail e si sceglie il bucket S3 denominato per ricevere i file di registro. `amzn-s3-demo-bucket1` Puoi quindi aggiornare il percorso per specificare che desideri registrare gli eventi di gestione e di dati Read (Lettura).
2. Crei un secondo trail e scegli il bucket S3 `amzn-s3-demo-bucket2` per ricevere i file di log. Puoi quindi aggiornare il percorso e specificare che desideri registrare gli eventi di gestione e di dati Write (Scrittura).
3. Le operazioni Amazon EC2 `DescribeInstances` e `TerminateInstances` API avvengono nel tuo account.
4. L'operazione API `DescribeInstances` è un evento di sola lettura e corrisponde alle impostazioni del primo trail. Il trail registra e distribuisce l'evento in `amzn-s3-demo-bucket1`.
5. L'operazione API `TerminateInstances` è un evento di sola scrittura e corrisponde alle impostazioni del secondo trail. Il trail registra e distribuisce l'evento in `amzn-s3-demo-bucket2`.

Registrazione degli eventi relativi ai dati con il AWS Management Console

Le seguenti procedure descrivono come aggiornare un datastore di eventi esistente o come tracciare gli eventi di dati utilizzando la AWS Management Console. Per ulteriori informazioni su come creare un datastore di eventi per registrare gli eventi di dati, consulta Crea un archivio dati di CloudTrail eventi per gli eventi con la console. Per ulteriori informazioni su come creare un percorso per registrare gli eventi di dati, consulta Creazione di un percorso con la console.

Per i percorsi, i passaggi per la registrazione degli eventi relativi ai dati variano a seconda che si utilizzino selettori di eventi avanzati o selettori di eventi di base. Puoi registrare eventi di dati per tutti i tipi di risorse utilizzando selettori di eventi avanzati, ma se utilizzi selettori di eventi di base sei limitato alla registrazione di eventi di dati per bucket Amazon S3 e oggetti bucket, AWS Lambda funzioni e tabelle Amazon DynamoDB.

Aggiornamento di un data store di eventi esistente per registrare gli eventi di dati utilizzando la console

Utilizza la seguente procedura per aggiornare un datastore di eventi esistente per registrare gli eventi di dati. Per ulteriori informazioni sull'utilizzo dei selettori di eventi avanzati, Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati consulta questo argomento.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione, in Lake seleziona Datastore di eventi.
3. Nella pagina Datastore di eventi, scegli il datastore di eventi che desideri aggiornare.

   > **Note**
   >
   > È possibile abilitare gli eventi relativi ai dati solo negli archivi dati di eventi che contengono CloudTrail eventi. Non è possibile abilitare eventi di dati nei data store di eventi per elementi di AWS Config configurazione, eventi CloudTrail Insights o non AWS eventi. CloudTrail

4. Nella pagina dei dettagli del percorso, in Eventi di dati scegli Modifica.
5. Se non stai già registrando eventi di dati, scegli la casella di controllo Data events (Eventi di dati).
6. Per Tipo di risorsa, scegli il tipo di risorsa su cui desideri registrare gli eventi relativi ai dati.
7. Scegli un modello di selettore di registro. Puoi scegliere un modello predefinito o scegliere Personalizzato per definire le condizioni di raccolta degli eventi.

Puoi scegliere tra i seguenti modelli predefiniti:

- Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
- Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
- Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
- Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
- Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

8. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
9. Se hai selezionato Personalizzato, in Advanced event selector crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

a. Scegli tra i seguenti campi.

   - **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.

- **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`
- **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.
- eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete
- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.`ARN, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.`ARN campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

b. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere gli eventi di dati per due bucket S3 dagli eventi di dati registrati nel tuo event data store, puoi impostare il campo su Resources.arn, impostare l'operatore for doesnot start con e quindi incollare un bucket S3 ARN per il quale non desideri registrare gli eventi.

   Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

c. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

10. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati. Ripeti i passaggi 6 di questo passaggio per configurare i selettori di eventi avanzati per un altro tipo di risorsa.
11. Dopo aver esaminato e verificato le tue scelte, scegli Salva modifiche.

Aggiornamento di un percorso esistente per registrare gli eventi relativi ai dati con selettori di eventi avanzati utilizzando la console

In AWS Management Console, se il percorso utilizza selettori di eventi avanzati, è possibile scegliere tra modelli predefiniti che registrano tutti gli eventi relativi ai dati su una risorsa selezionata. Dopo aver scelto un modello di selettore di log, puoi personalizzare il modello per includere solo gli eventi di dati che desideri visualizzare. Per ulteriori informazioni sull'utilizzo dei selettori di eventi avanzati, consulta Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati questo argomento.

1. Nelle pagine Dashboard o Trails della CloudTrail console, scegli il percorso che desideri aggiornare.
2. Nella pagina dei dettagli del percorso, in Eventi di dati scegli Modifica.
3. Se non stai già registrando eventi di dati, scegli la casella di controllo Data events (Eventi di dati).
4. Per Tipo di risorsa, scegli il tipo di risorsa su cui desideri registrare gli eventi relativi ai dati.
5. Scegli un modello di selettore di registro. Puoi scegliere un modello predefinito o scegliere Personalizzato per definire le condizioni di raccolta degli eventi.

Puoi scegliere tra i seguenti modelli predefiniti:

- Registra tutti gli eventi: scegli questo modello per registrare tutti gli eventi.
- Registra solo gli eventi di lettura: scegli questo modello per registrare solo gli eventi di lettura. Gli eventi di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio gli eventi `Get*` o`Describe*`.
- Registra solo gli eventi di scrittura: scegli questo modello per registrare solo gli eventi di scrittura. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`.
- Registra solo AWS Management Console eventi: scegli questo modello per registrare solo gli eventi provenienti da. AWS Management Console
- Escludi eventi Servizio AWS iniziati: scegli questo modello per escludere Servizio AWS gli eventi con un `eventType` off e gli eventi iniziati con Servizio AWS-linked roles (). `AwsServiceEvent` SLRs

> **Note**
>
> La scelta di un modello predefinito per i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket attualmente presenti nel tuo AWS account e per tutti i bucket che crei dopo aver completato la creazione del trail. Consente inoltre la registrazione delle attività relative agli eventi relativi ai dati eseguite da qualsiasi utente o ruolo nel tuo AWS account, anche se tale attività viene eseguita su un bucket che appartiene a un altro account. AWS
> Se il percorso è valido solo per una regione, la selezione di un modello predefinito che registra tutti i bucket S3 abilita la registrazione degli eventi di dati per tutti i bucket nella stessa regione del percorso e per qualsiasi bucket creato in seguito in tale regione. Non registrerà nel tuo account gli eventi relativi ai dati per i bucket Amazon S3 in altre regioni. AWS
> Se stai creando un percorso per tutte le regioni, la scelta di un modello predefinito per le funzioni Lambda abilita la registrazione degli eventi dei dati per tutte le funzioni attualmente presenti nel AWS tuo account e per tutte le funzioni Lambda che potresti creare in qualsiasi regione dopo aver completato la creazione del percorso. Se stai creando un percorso per una singola regione (per i sentieri, questa operazione può essere eseguita solo utilizzando il AWS CLI), questa selezione abilita la registrazione degli eventi dei dati per tutte le funzioni attualmente presenti in quella regione nel tuo

AWS account e per tutte le funzioni Lambda che potresti creare in quella regione dopo aver terminato la creazione del percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
La registrazione degli eventi relativi ai dati per tutte le funzioni consente inoltre di registrare l'attività degli eventi relativi ai dati eseguita da qualsiasi utente o ruolo nell' AWS account, anche se tale attività viene eseguita su una funzione che appartiene a un altro AWS account.

6. (Facoltativo) In Nome selettore inserisci un nome per identificare il selettore. Il nome del selettore è un nome descrittivo per un selettore di eventi avanzato, ad esempio "Registra eventi di dati solo per due bucket S3". Il nome del selettore è riportato come `Name` nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
7. Se hai selezionato Personalizzato, in Selettori di eventi avanzati crea un'espressione basata sui valori dei campi avanzati del selettore di eventi.

> **Note**
>
> I selettori non supportano l'uso di caratteri jolly come. `*` Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

   a. Scegli tra i seguenti campi.

      - **`readOnly`**- `readOnly` può essere impostato su un valore uguale a o. `true` `false` Gli eventi di dati di sola lettura sono eventi che non modificano lo stato di una risorsa, ad esempio eventi `Get*` o `Describe*`. Gli eventi di scrittura aggiungono, modificano o eliminano risorse, attributi o artefatti, ad esempio eventi `Put*`, `Delete*` oppure `Write*`. Per registrare sia eventi `read` che `write`, non aggiungere un selettore `readOnly`.
      - **`eventName`**: `eventName` può utilizzare qualsiasi operatore. È possibile utilizzarlo per includere o escludere qualsiasi evento relativo ai dati registrato CloudTrail, ad esempio`PutBucket`, `GetItem` o. `GetSnapshotBlock`
      - **`eventSource`**— L'origine dell'evento da includere o escludere. Questo campo può utilizzare qualsiasi operatore.
      - eventType — Il tipo di evento da includere o escludere. Ad esempio, è possibile impostare questo campo su non uguale `AwsServiceEvent` a escludere. Servizio AWS eventi Per

un elenco dei tipi di eventi, vedere `eventType`in. CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete

- sessionCredentialFromConsole: include o esclude eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su uguale o non uguale con un valore di. `true`
- UserIdentity.ARN: include o esclude eventi per le azioni intraprese da identità IAM specifiche. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .
- **`resources.ARN`**- È possibile utilizzare qualsiasi operatore con`resources.ARN`, ma se si utilizza uguale o diverso, il valore deve corrispondere esattamente all'ARN di una risorsa valida del tipo specificato nel modello come valore di. `resources.type`

> **Note**
>
> Non è possibile utilizzare il `resources.ARN` campo per filtrare i tipi di risorse che non sono disponibili. ARNs

Per ulteriori informazioni sui formati ARN delle risorse relative agli eventi di dati, vedere Azioni, risorse e chiavi di condizione Servizi AWS nel Service Authorization Reference.

b. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni. Ad esempio, per escludere gli eventi di dati per due bucket S3 dagli eventi di dati registrati nel tuo event data store, puoi impostare il campo su Resources.arn, impostare l'operatore for doesnot start con e quindi incollare un bucket S3 ARN per il quale non desideri registrare gli eventi.

   Per aggiungere il secondo bucket S3, scegli + Condizioni, quindi ripeti l'istruzione precedente, cercando un bucket diverso o incollandone l'ARN.

   CloudTrail Per Come CloudTrail valuta più condizioni per un campo informazioni su come valuta più condizioni, consulta.

> **Note**
>
> Puoi avere un massimo di 500 valori per tutti i selettori su un datastore di eventi. Questo include array di più valori per un selettore come `eventName`. Se disponi di

valori singoli per tutti i selettori, puoi avere un massimo di 500 condizioni aggiunte a un selettore.

c. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi. Ad esempio, non specificare l'ARN di un selettore come uguale a un valore, quindi specifica che l'ARN non è uguale allo stesso valore in un altro selettore.

8. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati. Ripeti i passaggi 4 di questo passaggio per configurare i selettori di eventi avanzati per il tipo di risorsa.
9. Dopo aver esaminato e verificato le tue scelte, scegli Salva modifiche.

Aggiorna un percorso esistente per registrare gli eventi relativi ai dati con selettori di eventi di base utilizzando la console

Utilizza la seguente procedura per aggiornare un percorso esistente per registrare gli eventi di dati utilizzando selettori di eventi di base.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Apri la pagina Percorsi della CloudTrail console e scegli il nome del percorso.

> **Note**
>
> Anche se è possibile modificare un percorso esistente per registrare gli eventi di dati, come best practice si consiglia di creare un percorso separato apposta per registrare gli eventi di dati.

3. Per Data events (Eventi di dati), scegli Edit (Modifica).
4. Per i bucket Amazon S3:

   a. Per Data event source (Origine evento di dati), scegli S3.

   b. Puoi scegliere di registrare All current and future S3 buckets (Tutti i bucket S3 attuali e futuri) oppure puoi specificare bucket o funzioni specifici. Per impostazione predefinita, gli eventi di dati vengono registrati per tutti i bucket S3 attuali e futuri.

> **Note**
>
> Mantenendo l'opzione predefinita Tutti i bucket S3 attuali e futuri, abilita la registrazione degli eventi di dati per tutti i bucket attualmente presenti nel tuo AWS account e per tutti i bucket che crei dopo aver completato la creazione del trail. Consente inoltre la registrazione delle attività relative agli eventi relativi ai dati eseguite da qualsiasi utente o ruolo nel tuo AWS account, anche se tale attività viene eseguita su un bucket che appartiene a un altro account. AWS
> Se stai creando un percorso per una singola regione (operazione eseguita utilizzando AWS CLI), la selezione dell'opzione Seleziona tutti i bucket S3 nel tuo account abilita la registrazione degli eventi relativi ai dati per tutti i bucket nella stessa regione del percorso e per tutti i bucket che creerai successivamente in quella regione. Non registrerà nel tuo account gli eventi relativi ai dati per i bucket Amazon S3 in altre regioni. AWS

c. Se lasci l'impostazione predefinita All current and future S3 buckets (Tutti i bucket S3 attuali e futuri), scegli di registrare gli eventi Read (Lettura), Write (Scrittura) o entrambi.

d. Per selezionare singoli bucket, deseleziona le caselle di controllo Read (Lettura) e Write (Scrittura) per All current and future S3 buckets (Tutti i bucket S3 attuali e futuri). In Individual bucket selection (Selezione di singoli bucket), cerca un bucket in cui registrare gli eventi di dati. Per trovare bucket specifici, digita un prefisso del bucket per il bucket desiderato. Puoi selezionare più bucket in questa finestra. Scegli Add bucket (Aggiungi bucket) per registrare eventi di dati per più bucket. Scegli di registrare gli eventi Read (Lettura), ad esempio `GetObject`, gli eventi Write (Scrittura), ad esempio `PutObject`, oppure entrambi.

   Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascun bucket. Ad esempio, se specifichi la registrazione degli eventi di lettura (Read) per tutti i buckets S3 e quindi scegli di aggiungere un bucket specifico per la registrazione degli eventi di dati, l'opzione Read (Lettura) è già selezionata per il bucket aggiunto. Non è possibile eliminare la selezione. Puoi solo configurare l'opzione Write (Scrittura).

   Per rimuovere un bucket dalla registrazione, scegli X.

5. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati.

6. Per le funzioni Lambda:

a. Per Data event source (Origine evento di dati), scegli Lambda.

b. In Lambda function (Funzione Lambda), scegli All regions (Tutte le regioni) per registrare tutte le funzioni Lambda o Input function as ARN (Inserire la funzione come ARN) per registrare eventi di dati su una funzione specifica.

   Per registrare gli eventi di dati per tutte le funzioni Lambda nell'account AWS , seleziona Log all current and future functions (Registra tutte le funzioni presenti e future). Questa impostazione ha la priorità sulle singole impostazioni configurate per ciascuna funzione. Tutte le funzioni vengono registrate, anche se tutte le funzioni non vengono visualizzate.

   > **Note**
   >
   > Se stai creando un percorso per tutte le regioni, questa selezione consente la registrazione degli eventi di dati per tutte le funzioni attualmente nell'account AWS e qualsiasi funzione Lambda che puoi creare in qualsiasi regione dopo aver creato il percorso. Se stai creando un percorso per una singola regione (eseguita utilizzando il AWS CLI), questa selezione abilita la registrazione degli eventi di dati per tutte le funzioni attualmente presenti in quella regione nel tuo AWS account e per tutte le funzioni Lambda che potresti creare in quella regione dopo aver terminato la creazione del percorso. Non viene abilitata la registrazione degli eventi di dati per le funzioni Lambda create in altre regioni.
   > La registrazione degli eventi relativi ai dati per tutte le funzioni consente inoltre di registrare le attività relative agli eventi relativi ai dati eseguite da qualsiasi utente o ruolo nell' AWS account, anche se tale attività viene eseguita su una funzione che appartiene a un altro account. AWS

c. Se scegli Input function as ARN (Inserire la funzione come ARN), immetti l'ARN di una funzione Lambda.

   > **Note**
   >
   > Se hai più di 15.000 funzioni Lambda nel tuo account, non puoi visualizzare o selezionare tutte le funzioni nella console durante CloudTrail la creazione di un trail. Puoi comunque selezionare l'opzione che consente di registrare tutte le funzioni, anche se non sono visualizzate. Se desideri registrare gli eventi di dati per funzioni specifiche, puoi aggiungere manualmente una funzione di cui conosci l'ARN. Puoi anche completare la creazione del percorso nella console e quindi utilizzare il AWS

CLI put-event-selectors comando and per configurare la registrazione degli eventi dei dati per funzioni Lambda specifiche. Per ulteriori informazioni, consulta Gestire i percorsi con AWS CLI.

7. Per aggiungere un altro tipo di risorsa su cui registrare gli eventi relativi ai dati, scegli Aggiungi tipo di evento dati.
8. Per le tabelle Dynamo DB:
   a. Per Data event source (Origine evento di dati), scegli Dynamo DB.
   b. In DynamoDB table selection (Selezione tabella Dynamo DB), scegli Browse (Sfoglia) per selezionare una tabella o incolla l'ARN di una tabella Dynamo DB a cui hai accesso. L'ARN di una tabella Dynamo DB ha il seguente formato:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   Per aggiungere un'altra tabella, scegli Add row (Aggiungi riga) e cerca una tabella o incolla l'ARN di una tabella a cui hai accesso.
9. Scegli Save changes (Salva modifiche).

Registrazione degli eventi relativi ai dati con AWS Command Line Interface

È possibile configurare i percorsi o i datastore di eventi per includere eventi di dati utilizzando la AWS CLI.

Argomenti

- Registrazione degli eventi relativi ai dati per i sentieri con il AWS CLI
- Registrazione degli eventi relativi ai dati per gli archivi dati degli eventi con AWS CLI

Registrazione degli eventi relativi ai dati per i sentieri con il AWS CLI

Puoi configurare i trail per registrare gli eventi di gestione e dati utilizzando la AWS CLI.

Note

- Tieni presente che se l'account registra più di una copia degli eventi di gestione, ti verranno addebitati i costi. È sempre previsto un addebito per la registrazione degli eventi di dati. Per ulteriori informazioni, consulta Prezzi di AWS CloudTrail.
- È possibile utilizzare selettori di eventi avanzati o selettori di eventi di base, ma non entrambi. Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti.
- Se il percorso utilizza selettori di eventi di base, è possibile registrare solo i seguenti tipi di risorse:
  - `AWS::DynamoDB::Table`
  - `AWS::Lambda::Function`
  - `AWS::S3::Object`

  Per registrare tipi di risorse aggiuntivi, è necessario utilizzare selettori di eventi avanzati. Per convertire un percorso a selettori di eventi avanzati, esegui il comando get-event-selectors per confermare i selettori di eventi correnti, quindi configura i selettori di eventi avanzati in modo che corrispondano alla copertura dei selettori di eventi precedenti. A questo punto, aggiungi i selettori per tutti i tipi di risorse per i quali desideri registrare gli eventi di dati.
- È possibile utilizzare selettori di eventi avanzati per filtrare in base al valore dei campi di selezione degli eventi avanzati supportati. I campi di selezione degli eventi avanzati supportati offrono la possibilità di registrare solo gli eventi di dati di interesse. Per ulteriori informazioni sulla configurazione di questi campi, consulta AdvancedFieldSelectorl'AWS CloudTrail API Reference e Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati questa guida.

Per verificare se il percorso sta registrando gli eventi di gestione e di dati, esegui il comando `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

Il comando restituisce i selettori di eventi per il trail.

Argomenti

- Registra gli eventi relativi ai dati per i percorsi utilizzando selettori di eventi avanzati
- Registra tutti gli eventi Amazon S3 per un bucket Amazon S3 utilizzando selettori di eventi avanzati
- Registrazione di eventi Amazon S3 su AWS Outposts utilizzando i selettori di eventi avanzati
- Registrazione di eventi utilizzando i selettori di eventi di base

Registra gli eventi relativi ai dati per i percorsi utilizzando selettori di eventi avanzati

> **Note**
>
> Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti. Prima di configurare i selettori di eventi avanzati, esegui il comando get-event-selectors per confermare i selettori di eventi correnti, quindi configura i selettori di eventi avanzati in modo che corrispondano alla copertura dei selettori di eventi precedenti. A questo punto, aggiungi i selettori per gli eventuali eventi di dati aggiuntivi che vuoi registrare.

L'esempio seguente crea selettori di eventi avanzati personalizzati per un percorso denominato in *`TrailName`* modo da includere eventi di gestione di lettura e scrittura (omettendo il `readOnly` selettore) `PutObject` ed eventi di `DeleteObject` dati per tutte le combinazioni bucket/prefisso di Amazon S3 ad eccezione di un bucket denominato ed eventi dati per una funzione denominata. `amzn-s3-demo-bucket` AWS Lambda `MyLambdaFunction` Poiché si tratta di selettori di eventi avanzati personalizzati, ogni set di selettori ha un nome descrittivo. Nota che una barra finale fa parte del valore ARN per i bucket S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
```

```
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

L'esempio restituisce i selettori di eventi avanzati configurati per il percorso.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::amzn-s3-demo-bucket/" ]
```

```
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Registra tutti gli eventi Amazon S3 per un bucket Amazon S3 utilizzando selettori di eventi avanzati

> **Note**
>
> Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti.

L'esempio seguente mostra come configurare il percorso per includere tutti gli eventi di dati per tutti gli oggetti Amazon S3 in un S3 Bucket specifico. Il valore per gli eventi S3 per il campo `resources.type` è `AWS::S3::Object`. Poiché i valori ARN per gli oggetti S3 e i bucket S3 sono leggermente diversi, devi aggiungere l'operatore `StartsWith` affinché `resources.ARN` acquisisca tutti gli eventi.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] }
            ]
        }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::amzn-s3-demo-bucket/"
                    ]
                }
            ]
        }
    ]
```

```
}
```

Registrazione di eventi Amazon S3 su AWS Outposts utilizzando i selettori di eventi avanzati

> **Note**
>
> Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti.

L'esempio seguente mostra come configurare il percorso per includere tutti gli eventi di dati per tutti gli oggetti Amazon S3 su Outposts nell'outpost.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
```

```
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

Registrazione di eventi utilizzando i selettori di eventi di base

Di seguito è riportato un risultato di esempio del comando get-event-selectors, che mostra i selettori di eventi di base. Per impostazione predefinita, quando crei un percorso utilizzando il AWS CLI, un trail registra tutti gli eventi di gestione. Per impostazione predefinita, i trail non registrano gli eventi di dati

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

Per configurare il percorso per registrare gli eventi di gestione e di dati, esegui il comando put-event-selectors.

L'esempio seguente mostra come utilizzare i selettori di eventi di base per configurare il percorso in modo da includere tutti gli eventi di gestione e gli eventi di dati per gli oggetti S3 in due prefissi di bucket S3. Puoi specificare da 1 a 5 selettori di eventi per un trail. Puoi specificare da 1 a 250 risorse di dati per un trail.

> **Note**
>
> Il numero massimo di risorse di dati S3 è 250, se scegli di limitare gli eventi di dati utilizzando selettori di eventi di base.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-demo-bucket1/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2;/prefix2"] }] }]'
```

Il comando restituisce i selettori di eventi configurati per il percorso.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket1/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

Registrazione degli eventi relativi ai dati per gli archivi dati degli eventi con AWS CLI

È possibile configurare i datastore di eventi per includere eventi di dati utilizzando la AWS CLI. Utilizza il comando `create-event-data-store` per creare un nuovo datastore di eventi registrare gli eventi di dati. Utilizza il comando `update-event-data-store` per aggiornare i selettori di eventi avanzati per un datastore di eventi esistente.

È possibile configurare selettori di eventi avanzati per registrare gli eventi di dati su un archivio dati di eventi. Per un elenco dei campi supportati, consultaFiltraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati.

Per vedere se il datastore di eventi include eventi di gestione, esegui il comando `get-event-data-store`.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

Il comando restituisce le impostazioni per il datastore di eventi.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

Argomenti

- Includi tutti gli eventi Amazon S3 per un bucket specifico
- Inclusione di Amazon S3 negli eventi AWS Outposts

Includi tutti gli eventi Amazon S3 per un bucket specifico

L'esempio seguente mostra come creare un data store di eventi per includere tutti gli eventi di dati per tutti gli oggetti Amazon S3 in uno specifico bucket S3 generico ed escludere Servizio AWS eventi ed eventi generati da. `bucket-scanner-role` `userIdentity` Il valore per gli eventi S3 per il campo `resources.type` è `AWS::S3::Object`. Poiché i valori ARN per gli oggetti S3 e i bucket S3 sono leggermente diversi, devi aggiungere l'operatore `StartsWith` affinché `resources.ARN` acquisisca tutti gli eventi.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]},
            { "Field": "eventType","NotEquals": ["AwsServiceEvent"]}
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
```

```
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::amzn-s3-demo-bucket/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                     ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2024-11-20T20:49:21.766000+00:00"
}
```

Inclusione di Amazon S3 negli eventi AWS Outposts

L'esempio seguente mostra come creare un datastore di eventi che include tutti gli eventi di dati per tutti gli oggetti Amazon S3 su Outposts nell'outpost.

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
```

```
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

Filtraggio degli eventi relativi ai dati utilizzando selettori di eventi avanzati

Questa sezione descrive come utilizzare selettori di eventi avanzati per creare selettori dettagliati per la registrazione degli eventi relativi ai dati, che possono aiutarti a controllare i costi registrando solo gli eventi di dati specifici di interesse.

Per esempio:

- È possibile includere o escludere chiamate API specifiche aggiungendo un filtro sul campo. `eventName`
- Puoi includere o escludere la registrazione per risorse specifiche aggiungendo un filtro sul `resources.ARN` campo. Ad esempio, se stavi registrando gli eventi relativi ai dati S3, potresti escludere la registrazione per il bucket S3 del tuo percorso.
- Puoi scegliere di registrare solo gli eventi di sola scrittura o gli eventi di sola lettura aggiungendo un filtro sul campo. `readOnly`

La tabella seguente descrive i campi supportati per il filtraggio degli eventi relativi ai dati. Per un elenco dei campi supportati per ogni tipo di CloudTrail evento, consulta AdvancedEventSelectorl'AWS CloudTrail API Reference.

Campo	Richiesto	Operatori validi	Descrizione
`eventCategory`	Sì	`Equals`	Questo campo è impostato per registrar e `Data` gli eventi relativi ai dati.
`resources.type`	Sì	`Equals`	Questo campo viene utilizzato per selezionare il tipo di risorsa per cui si desidera registrare gli eventi relativi ai dati. La tabella Data events mostra i valori possibili.
`readOnly`	No	`Equals`	Questo è un campo opzionale utilizzato per includere o escludere eventi relativi

Campo	Richiesto	Operatori validi	Descrizione
			ai dati in base al `readOnly` valore. Un valore di `true` log legge solo gli eventi. Un valore di `false` log scrive solo eventi. Se non si aggiunge questo campo, CloudTrail registra sia gli eventi di lettura che quelli di scrittura.

`eventName`	No	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Si tratta di un campo opzionale utilizzato per filtrare o filtrare qualsiasi evento relativo ai dati registrato, ad esempio o. CloudTrail `PutBucket` `GetSnapshotBlock`
			
			Se utilizzi il AWS CLI, puoi specificare più valori separando ogni valore con una virgola.
			
			Se utilizzi la console, puoi specificare più valori creando una condizione per ognuno dei quali `eventName` desideri filtrare.

Campo	Richiesto	Operatori validi	Descrizione

`resources.ARN`	No	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Questo è un campo facoltativo utilizzato per escludere o includere eventi di dati per una risorsa specifica fornendo il `resources.ARN`. È possibile utilizzare qualsiasi operatore con `resources.ARN`, ma se si utilizza `Equals` o `NotEquals`, il valore deve corrispondere esattamente all'ARN di una risorsa valida per il valore `resources.type` specificato. Per registrare tutti gli eventi di dati per tutti gli oggetti in un bucket S3 specifico, utilizza l'operatore `StartsWith` e includi solo l'ARN del bucket come valore corrispondente.
			
			Se utilizzi il AWS CLI, puoi specificare più valori separando ogni valore con una virgola.
			
			Se utilizzi la console, puoi specificare più valori creando una condizione per ognuno dei quali `resources.ARN` desideri filtrare.

Campo	Richiesto	Operatori validi	Descrizione

`eventSource`	No	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Puoi usarla per includere o escludere fonti di eventi specifiche. In genere `eventSource` è una forma abbreviata del nome del servizio senza spazi plus `.amazonaws.com`. Ad esempio, puoi impostare la registrazione solo degli eventi EC2 relativi `eventSource` `Equals` `ec2.amazonaws.com` ai dati di Amazon.

`eventType`	No	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			L'EventType da includere o escludere. Ad esempio, è possibile impostare questo campo su per `NotEquals` `AwsServiceEvent` escludere Servizio AWS gli eventi.

`sessionCredentialFromConsole`	No	`Equals` `NotEquals`	Includi o escludi eventi provenienti da una AWS Management Console sessione. Questo campo può essere impostato su `Equals` o `NotEquals` con un valore di`true`.

Campo	Richiesto	Operatori validi	Descrizione

`userIdentity.arn`	No	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Includi o escludi eventi per le azioni intraprese da identità IAM specifich e. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .

Per registrare gli eventi relativi ai dati utilizzando la CloudTrail console, scegli l'opzione Data events e quindi seleziona il tipo di risorsa che ti interessa quando crei o aggiorni un trail o un data store di eventi. La tabella Data events mostra i possibili tipi di risorse che puoi scegliere sulla CloudTrail console.

Per registrare gli eventi relativi ai dati con AWS CLI, configura il `--advanced-event-selector` parametro in modo che imposti `eventCategory` un `resources.type` valore uguale `Data` e uguale al valore del tipo di risorsa per il quale desideri registrare gli eventi relativi ai dati. La tabella Data events elenca i tipi di risorse disponibili.

Ad esempio, se desideri registrare gli eventi relativi ai dati per tutti i pool di identità di Cognito, devi configurare il `--advanced-event-selectors` parametro in questo modo:

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
```

```
    }
]'
```

L'esempio precedente registra tutti gli eventi relativi ai dati di Cognito nei pool di identità. È possibile perfezionare ulteriormente i selettori di eventi avanzati per filtrare in base ai `resources.`ARN campi `eventNameread0nly`, e per registrare eventi specifici di interesse o escludere eventi che non sono di interesse.

Puoi configurare selettori di eventi avanzati per filtrare gli eventi di dati in base a più campi. Ad esempio, puoi configurare selettori di eventi avanzati per registrare tutte le chiamate Amazon `PutObject` S3 `DeleteObject` e API, ma escludere la registrazione degli eventi per uno specifico bucket S3, come mostrato nell'esempio seguente. Sostituisci *`amzn-s3-demo-bucket`* con il nome del tuo bucket.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  }
]'
```

Puoi anche includere più condizioni per un campo. Per informazioni su come vengono valutate più condizioni, vedereCome CloudTrail valuta più condizioni per un campo.

È possibile utilizzare selettori di eventi avanzati per registrare sia gli eventi di gestione che quelli relativi ai dati. Per registrare gli eventi relativi ai dati per più tipi di risorse, aggiungi un'istruzione di selezione dei campi per ogni tipo di risorsa per cui desideri registrare gli eventi relativi ai dati.

> **Note**
>
> I trail possono utilizzare selettori di eventi di base o selettori di eventi avanzati, ma non entrambi. Se si applicano selettori di eventi avanzati a un percorso, tutti i selettori di eventi di base esistenti vengono sovrascritti.

I selettori non supportano l'uso di caratteri jolly come. * Per abbinare più valori a una singola condizione, puoi usare`StartsWith`, `EndsWithNotStartsWith`, o `NotEndsWith` far corrispondere esplicitamente l'inizio o la fine del campo dell'evento.

Argomenti

- Come CloudTrail valuta più condizioni per un campo
- AWS CLI esempi per filtrare gli eventi relativi ai dati

Come CloudTrail valuta più condizioni per un campo

Per i selettori di eventi avanzati, CloudTrail valuta più condizioni per un campo nel modo seguente:

- Gli operatori DESELECT vengono uniti in modalità AND. Se una qualsiasi delle condizioni dell'operatore DESELECT è soddisfatta, l'evento non viene consegnato. Questi sono gli operatori DESELECT validi per i selettori di eventi avanzati:
  - `NotEndsWith`
  - `NotEquals`
  - `NotStartsWith`
- Gli operatori SELECT vengono combinati in OR. Questi sono gli operatori SELECT validi per i selettori di eventi avanzati:
  - `EndsWith`
  - `Equals`
  - `StartsWith`
- Le combinazioni degli operatori SELECT e DESELECT seguono le regole precedenti ed entrambi i gruppi vengono combinati in AND.

Esempio che mostra più condizioni per il campo **`resources.ARN`**

L'istruzione di selezione degli eventi di esempio seguente raccoglie gli eventi di dati per il tipo di `AWS::S3::Object` risorsa e applica più condizioni sul `resources.`ARN campo.

```
{
    "Name": "S3Select",
    "FieldSelectors": [
      {
```

```
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "resources.ARN",
        "Equals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object1"
        ],
        "StartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "EndsWith": [
          "object3"
        ],
        "NotStartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/deselect"
        ],
        "NotEndsWith": [
          "object5"
        ],
        "NotEquals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object6"
        ]
      }
    ]
  }
```

Nell'esempio precedente, gli eventi relativi ai dati di Amazon S3 per `AWS::S3::Object` la risorsa verranno consegnati se:

1. Nessuna di queste condizioni dell'operatore DESELECT è soddisfatta:
   - il `resources.ARN` campo `NotStartsWith` il valore `arn:aws:s3:::amzn-s3-demo-bucket/deselect`
   - il `resources.ARN` campo `NotEndsWith` il valore `object5`

- il `resources.ARN` campo `NotEquals` il valore `arn:aws:s3:::amzn-s3-demo-bucket/object6`

2. È soddisfatta almeno una di queste condizioni dell'operatore SELECT:
   - il `resources.ARN` campo `Equals` il valore `arn:aws:s3:::amzn-s3-demo-bucket/object1`
   - il `resources.ARN` campo `StartsWith` il valore `arn:aws:s3:::amzn-s3-demo-bucket/`
   - il `resources.ARN` campo `EndsWith` il valore `object3`

In base alla logica di valutazione:

1. Gli eventi di dati per `amzn-s3-demo-bucket/object1` verranno consegnati perché corrispondono al valore per l'`Equals`operatore e non corrispondono a nessuno dei valori per gli `NotEquals` operatori `NotStartsWithNotEndsWith`, e.
2. L'evento di dati per `amzn-s3-demo-bucket/object2` verrà fornito perché corrisponde al valore per l'`StartsWith`operatore e non corrisponde a nessuno dei valori per gli `NotEquals` operatori `NotStartsWithNotEndsWith`, e.
3. Gli eventi di dati per `amzn-s3-demo-bucket1/object3` verranno consegnati perché corrispondono all'`EndsWith`operatore e non corrispondono a nessuno dei valori `NotEquals` degli operatori `NotStartsWithNotEndsWith`, e.
4. Gli eventi relativi ai dati di non `arn:aws:s3:::amzn-s3-demo-bucket/deselectObject4` verranno consegnati perché corrispondono alla condizione di, `NotStartsWith` anche se corrispondono alla condizione dell'`StartsWith`operatore.
5. Gli eventi relativi ai dati di non `arn:aws:s3:::amzn-s3-demo-bucket/object5` verranno consegnati perché corrispondono alla condizione di, `NotEndsWith` anche se corrispondono alla condizione dell'`StartsWith`operatore.
6. Gli eventi relativi ai dati non `arn:aws:s3:::amzn-s3-demo-bucket/object6` verranno consegnati perché corrispondono alla condizione dell'`NotEquals`operatore anche se corrisponde alla condizione dell'`StartsWith`operatore.

AWS CLI esempi per filtrare gli eventi relativi ai dati

Questa sezione fornisce AWS CLI esempi che mostrano come filtrare gli eventi relativi ai dati su campi diversi. Per ulteriori AWS CLI esempi, vedere Registra gli eventi relativi ai dati per i percorsi

utilizzando selettori di eventi avanzati eRegistrazione degli eventi relativi ai dati per gli archivi dati degli eventi con AWS CLI.

Per informazioni su come registrare gli eventi relativi ai dati utilizzando la console, vedereRegistrazione degli eventi relativi ai dati con il AWS Management Console.

Esempi:

- Esempio 1: filtraggio sul campo eventName
- Esempio 2: filtraggio in base ai campi resources.ARN e userIdentity.arn
- Esempio 3: filtraggio sui eventName campi resources.type and per escludere singoli oggetti eliminati da un evento Amazon DeleteObjects S3

Esempio 1: filtraggio sul campo **`eventName`**

Nel primo esempio, i `--advanced-event-selectors` for a trail sono configurati per registrare solo le chiamate `GetObjectPutObject`, e `DeleteObject` API per gli oggetti Amazon S3 in bucket generici.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

Il prossimo esempio crea un nuovo archivio dati di eventi che registra gli eventi di dati per EBS Direct APIs ma esclude le chiamate API. `ListChangedBlocks` È possibile utilizzare il update-event-data-storecomando per aggiornare un archivio dati di eventi esistente.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
```

```
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

Esempio 2: filtraggio in base ai campi **`resources.ARN`** e **`userIdentity.arn`**

L'esempio seguente mostra come includere tutti gli eventi relativi ai dati per tutti gli oggetti Amazon S3 in uno specifico bucket S3 generico ma escludere gli eventi generati da. `bucket-scanner-role` `userIdentity` Il valore per gli eventi S3 per il campo `resources.type` è `AWS::S3::Object`. Poiché i valori ARN per gli oggetti S3 e i bucket S3 sono leggermente diversi, è necessario aggiungere l'operatore per. `StartsWith` `resources.ARN`

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

Esempio 3: filtraggio sui **`eventName`** campi **`resources.type`** and per escludere singoli oggetti eliminati da un evento Amazon DeleteObjects S3

L'esempio seguente mostra come includere tutti gli eventi relativi ai dati per tutti gli oggetti Amazon S3 in uno specifico bucket Amazon S3 generico ma escludere i singoli oggetti eliminati dall'operazione. `DeleteObject` Il valore per gli eventi S3 per il campo `resources.type` è `AWS::S3::Object`. Il valore per il nome dell'evento è. `DeleteObject`

```
aws cloudtrail put-event-selectors \
```

```
--trail-name trailName \
--advanced-event-selectors \

{
    "Name": "Exclude Events for DeleteObject operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "NotEquals": [
          "DeleteObject"
        ]
      }
    ]
  },
  {
    "Name": "Exclude DeleteObject Events for individual objects deleted by
 DeleteObjects Operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
```

```
        "Equals": [
          "DeleteObject"
        ]
      },
      {
        "Field": "eventType",
        "NotEquals": [
          "AwsServiceEvent"
        ]
      }
    ]
  }
] (edited)
```

Registrazione di eventi di dati per la conformità di AWS Config

Se utilizzi pacchetti di AWS Config conformità per aiutare la tua azienda a mantenere la conformità a standard formalizzati come quelli richiesti dal Federal Risk and Authorization Management Program (FedRAMP) o dal National Institute of Standards and Technology (NIST), i pacchetti di conformità per i framework di conformità in genere richiedono almeno la registrazione degli eventi di dati per i bucket Amazon S3. I pacchetti di conformità per i framework di conformità includono una regola gestita chiamata `cloudtrail-s3-dataevents-enabled`, che controlla la registrazione degli eventi di dati S3 nell'account. Anche molti pacchetti di conformità non sono associati a framework di conformità richiedono la registrazione degli eventi di dati S3. Di seguito sono riportati esempi di pacchetti di conformità che includono questa regola.

- Best practice operative per AWS Well-Architected Framework Security Pillar
- Best practice operative per FDA Titolo 21 CFR Parte 11
- Best practice operative per FFIEC
- Best practice operative per FedRAMP (Moderato)
- Best practice operative per la sicurezza HIPAA
- Best practice operative per K-ISMS
- Best practice operative per la registrazione

Per un elenco completo dei pacchetti di conformità di esempio disponibili in AWS Config, consulta i modelli di esempio dei pacchetti di conformità nella Guida per gli sviluppatori.AWS Config

Registrazione degli eventi relativi ai dati con AWS SDKs

Esegui l'GetEventSelectorsoperazione per vedere se il tuo percorso sta registrando gli eventi relativi ai dati. È possibile configurare i percorsi per registrare gli eventi relativi ai dati eseguendo l'PutEventSelectorsoperazione. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS CloudTrail.

Esegui l'GetEventDataStoreoperazione per vedere se il tuo Event Data Store sta registrando gli eventi relativi ai dati. È possibile configurare i data store degli eventi per includere eventi di dati eseguendo UpdateEventDataStorele operazioni CreateEventDataStoreo e specificando selettori di eventi avanzati. Per ulteriori informazioni, consulta Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI e il Riferimento API di AWS CloudTrail.

Registrazione degli eventi delle attività di rete

CloudTrail gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Gli eventi di attività di rete forniscono visibilità sulle operazioni sulle risorse eseguite all'interno di un VPC. Ad esempio, la registrazione degli eventi delle attività di rete può aiutare i proprietari di endpoint VPC a rilevare quando credenziali esterne all'organizzazione tentano di accedere ai propri endpoint VPC.

È possibile registrare gli eventi di attività di rete per i seguenti servizi:

- AWS AppConfig
- AWS B2B Data Interchange
- Gestione dei costi e fatturazione
- Calcolatore dei prezzi AWS
- AWS Cost Explorer
- AWS CloudHSM
- Amazon Comprehend Medical
- AWS CloudTrail
- Esportazioni di dati AWS
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service

- Amazon EventBridge Scheduler
- Piano gratuito di AWS
- Amazon FSx
- AWS IoT FleetWise
- Fatturazione AWS
- AWS KMS
- AWS Lambda
- Amazon Lookout per le apparecchiature
- Amazon Rekognition
- Amazon S3

> **Note**
>
> I punti di accesso multi-regione Amazon S3 non sono supportati.

- AWS Secrets Manager
- Strumento di gestione degli incidenti AWS Systems Manager
- Amazon Textract
- Amazon WorkMail

È possibile configurare i percorsi o i datastore di eventi per registrare gli eventi di attività di rete.

Per impostazione predefinita, i percorsi e i datastore di eventi non registrano gli eventi di rete. Per gli eventi di rete sono previsti costi aggiuntivi. Per ulteriori informazioni, consultare AWS CloudTrail Prezzi.

Indice

- Campi avanzati di selezione degli eventi per gli eventi di attività di rete
- Registrazione degli eventi relativi alle attività di rete con AWS Management Console
  - Aggiornamento di un percorso esistente per registrare gli eventi di attività di rete
  - Aggiornamento di un datastore di eventi esistente per registrare gli eventi di attività di rete
- Registrazione degli eventi di attività di rete con AWS Command Line Interface
  - Esempi: Registrazione degli eventi di rete per i percorsi
    - Esempio: registra gli eventi di attività di rete per le operazioni CloudTrail

    - Esempio: registra VpceAccessDenied gli eventi per AWS KMS
    - Esempio: Registrazione di VpceAccessDenied eventi di registrazione per Amazon S3
    - Esempio: registra EC2 VpceAccessDenied gli eventi su un endpoint VPC specifico
    - Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi
  - Esempi: Registrazione degli eventi di rete per i datastore di eventi
    - Esempio: registra tutti gli eventi di attività di rete per CloudTrail le operazioni
    - Esempio: registra VpceAccessDenied gli eventi per AWS KMS
    - Esempio: registra EC2 VpceAccessDenied gli eventi su un endpoint VPC specifico
    - Esempio: Registrazione di VpceAccessDenied eventi di registrazione per Amazon S3
    - Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi
- Registrazione degli eventi con AWS SDKs

Campi avanzati di selezione degli eventi per gli eventi di attività di rete

È possibile configurare i selettori di eventi avanzati per registrare gli eventi di attività di rete specificando l'origine dell'evento per cui si desidera registrare l'attività. È possibile configurare selettori di eventi avanzati utilizzando la console AWS SDKs AWS CLI, o. CloudTrail

I seguenti campi avanzati di selezione degli eventi sono necessari per registrare gli eventi delle attività di rete:

- `eventCategory`— Per registrare gli eventi di attività di rete, il valore deve essere`NetworkActivity`. `eventCategory`può usare solo l'`Equals`operatore.
- `eventSource`— La fonte di eventi per la quale si desidera che registri gli eventi di attività di rete. `eventSource`può utilizzare solo l'`Equals`operatore. Se si desidera registrare gli eventi delle attività di rete per più fonti di eventi, è necessario creare un selettore di campo separato per ciascuna fonte di eventi.

  I valori validi includono:

  - `appconfig.amazonaws.com`
  - `b2bi.amazonaws.com`
  - `bcm-data-exports.amazonaws.com`
  - `bcm-pricing-calculator.amazonaws.com`
  - `billing.amazonaws.com`

- `ce.amazonaws.com`
- `cloudhsm.amazonaws.com`
- `cloudtrail.amazonaws.com`
- `comprehendmedical.amazonaws.com`
- `dynamodb.amazonaws.com`
- `ec2.amazonaws.com`
- `ecs.amazonaws.com`
- `freetier.amazonaws.com`
- `fsx.amazonaws.com`
- `invoicing.amazonaws.com`
- `iotfleetwise.amazonaws.com`
- `kms.amazonaws.com`
- `lambda.amazonaws.com`
- `lookoutequipment.amazonaws.com`
- `rekognition.amazonaws.com`
- `s3.amazonaws.com`
- `scheduler.amazonaws.com`
- `secretsmanager.amazonaws.com`
- `ssm-contacts.amazonaws.com`
- `textract.amazonaws.com`
- `workmail.amazonaws.com`

I seguenti campi avanzati di selezione degli eventi sono facoltativi:

- `eventName`— L'azione richiesta in base alla quale si desidera filtrare. Ad esempio, `CreateKey` o`ListKeys`. `eventName`può utilizzare qualsiasi operatore.
- `errorCode`— Il codice di errore richiesto in base al quale si desidera filtrare. Attualmente, l'unico valido `errorCode` è`VpceAccessDenied`. È possibile utilizzare solo l'`Equals`operatore con`errorCode`.
- `vpcEndpointId`— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con `vpcEndpointId`.

Quando si crea un percorso o un datastore di eventi, gli eventi di rete non vengono registrati per impostazione predefinita. Per registrare gli eventi di CloudTrail rete, devi configurare in modo esplicito ogni fonte di eventi per la quale desideri raccogliere le attività.

Per la registrazione di eventi di attività di rete sono previsti costi aggiuntivi. Per CloudTrail informazioni sui prezzi, consulta la sezione AWS CloudTrail Prezzi.

Registrazione degli eventi relativi alle attività di rete con AWS Management Console

È possibile aggiornare un percorso esistente o un datastore di eventi per registrare gli eventi di attività di rete utilizzando la console.

Argomenti

- Aggiornamento di un percorso esistente per registrare gli eventi di attività di rete
- Aggiornamento di un datastore di eventi esistente per registrare gli eventi di attività di rete

Aggiornamento di un percorso esistente per registrare gli eventi di attività di rete

Utilizza la seguente procedura per aggiornare un percorso esistente per registrare gli eventi di attività di rete.

> **Note**
>
> Per la registrazione di eventi di attività di rete sono previsti costi aggiuntivi. Per i prezzi CloudTrail, consulta Prezzi di AWS CloudTrail.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel pannello di navigazione a sinistra della CloudTrail console, apri la pagina Percorsi e scegli il nome del percorso.
3. Se il tuo percorso registra gli eventi relativi ai dati utilizzando selettori di eventi di base, dovrai passare ai selettori di eventi avanzati per registrare gli eventi delle attività di rete.

   Segui questi passaggi per passare ai selettori di eventi avanzati:

a. Nell'area Data events, prendi nota degli attuali selettori di eventi relativi ai dati. Il passaggio ai selettori di eventi avanzati eliminerà tutti i selettori di eventi di dati esistenti.

b. Scegliete Modifica, quindi scegliete Passa ai selettori di eventi avanzati.

c. Riapplica le selezioni degli eventi relativi ai dati utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Aggiornamento di un percorso esistente per registrare gli eventi relativi ai dati con selettori di eventi avanzati utilizzando la console.

4. In Eventi di attività di rete, scegli Modifica.

   Per registrare gli eventi di attività di rete, procedi come indicato di seguito:

   a. Da Origine degli eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.

   b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.

   c. (Facoltativo) Immetti un nome per identificare il selettore. Il nome del selettore è riportato come Name nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.

   d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

      i. Per escludere o includere eventi di rete, puoi scegliere tra i seguenti campi nella console.

         - **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi utilizzarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
         - **`errorCode`**— È possibile utilizzarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.
         - **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

      ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

      iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

   e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

5. Per salvare le modifiche, scegliere Salva modifiche.

Aggiornamento di un datastore di eventi esistente per registrare gli eventi di attività di rete

Utilizza la seguente procedura per aggiornare un datastore di eventi esistente per registrare gli eventi di attività di rete.

> **Note**
>
> È possibile registrare gli eventi di attività di rete solo nei data store di eventi di tipo CloudTrail eventi.

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione a sinistra della CloudTrail console, sotto Lake, scegli Event data stores.
3. Scegli l'evento dal datastore di eventi.
4. In Eventi di attività di rete, scegli Modifica.

   Per registrare gli eventi di attività di rete, procedi come indicato di seguito:

   a. Da Origine degli eventi di attività di rete, scegli la fonte per gli eventi di attività di rete.
   b. In Modello di selettore di log, scegliere un modello. Puoi scegliere di registrare tutti gli eventi di attività di rete, registrare tutti gli eventi di accesso negato all'attività di rete o scegliere Personalizzato per creare un selettore di registro personalizzato per filtrare più campi, come `eventName` `evpcEndpointId`.
   c. (Facoltativo) Immetti un nome per identificare il selettore. Il nome del selettore è riportato come Name nel selettore di eventi avanzato ed è visualizzabile se espandi la vista JSON.
   d. In Advanced, i selettori di eventi creano espressioni scegliendo i valori per Field, Operator e Value. Se utilizzi un modello di log predefinito, puoi ignorare questa fase.

i. Per escludere o includere eventi di rete, puoi scegliere tra i seguenti campi nella console.

- **`eventName`**— È possibile utilizzare qualsiasi operatore con`eventName`. Puoi utilizzarlo per includere o escludere qualsiasi evento, ad esempio`CreateKey`.
- **`errorCode`**— È possibile utilizzarlo per filtrare in base a un codice di errore. Attualmente, l'unico supportato `errorCode` è`VpceAccessDenied`.
- **`vpcEndpointId`**— Identifica l'endpoint VPC attraversato dall'operazione. È possibile utilizzare qualsiasi operatore con. `vpcEndpointId`

ii. Per ogni campo, scegliere + Condizioni per aggiungere tutte le condizioni necessarie, fino a un massimo di 500 valori specificati per tutte le condizioni.

iii. Scegli + Field (+ Campo) per aggiungere campi aggiuntivi in base alle necessità. Per evitare errori, non impostare valori in conflitto o duplicati per i campi.

e. Per aggiungere un'altra fonte di eventi per la quale desideri registrare gli eventi di attività di rete, scegli Aggiungi selettore di eventi di attività di rete.

f. Come opzione, espandere JSON view (Visualizzazione JSON) per vedere i propri selettori di eventi avanzati come un blocco JSON.

5. Per salvare le modifiche, scegliere Salva modifiche.

Registrazione degli eventi di attività di rete con AWS Command Line Interface

Puoi configurare i percorsi o i datastore di eventi per registrare gli eventi di attività di rete utilizzando la AWS CLI.

Argomenti

- Esempi: Registrazione degli eventi di rete per i percorsi
- Esempi: Registrazione degli eventi di rete per i datastore di eventi

Esempi: Registrazione degli eventi di rete per i percorsi

Puoi configurare i percorsi per la registrazione di eventi di attività di rete utilizzando la AWS CLI. Esegui il put-event-selectorscomando per configurare i selettori di eventi avanzati per il tuo percorso.

Per vedere se il percorso sta registrando eventi di attività di rete, esegui il `get-event-selectors`comando.

Argomenti

- Esempio: registra gli eventi di attività di rete per le operazioni CloudTrail
- Esempio: registra VpceAccessDenied gli eventi per AWS KMS
- Esempio: Registrazione di VpceAccessDenied eventi di registrazione per Amazon S3
- Esempio: registra EC2 VpceAccessDenied gli eventi su un endpoint VPC specifico
- Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi

Esempio: registra gli eventi di attività di rete per le operazioni CloudTrail

L'esempio seguente mostra come configurare il percorso per includere tutti gli eventi di rete per le operazioni delle CloudTrail API, ad esempio le chiamate di rete, ad esempio `CreateTrail` le `CreateEventDataStore` chiamate di rete. Il valore per il `eventSource` campo è`cloudtrail.amazonaws.com`.

```
aws cloudtrail put-event-selectors /
--trail-name TrailName /
--region region /
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit all CloudTrail API calls through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

Esempio: registra **`VpceAccessDenied`** gli eventi per AWS KMS

L'esempio seguente mostra come configurare il percorso per includere `VpceAccessDenied` eventi per AWS KMS. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi e il `eventSource` campo uguale a`kms.amazonaws.com`.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
```

```
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

Esempio: Registrazione di **`VpceAccessDenied`** eventi di registrazione per Amazon S3

L'esempio seguente mostra come configurare il percorso per includere `VpceAccessDenied` eventi per Amazon S3. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi e il `eventSource` campo uguale a`s3.amazonaws.com`.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

Esempio: registra EC2 **`VpceAccessDenied`** gli eventi su un endpoint VPC specifico

L'esempio seguente mostra come configurare il percorso per includere `VpceAccessDenied` eventi per Amazon EC2 per un endpoint VPC specifico. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi, il `eventSource` campo uguale e `vpcEndpointId` uguale all'endpoint VPC di interesse. `ec2.amazonaws.com`

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
```

```
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ]
```

```
}
```

Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi

L'esempio seguente configura un percorso per registrare gli eventi di gestione e tutti gli eventi di attività di rete per le sorgenti di eventi Amazon CloudTrail EC2 AWS KMS AWS Secrets Manager, e Amazon S3.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
```

```
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
```

```
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
```

```
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
```

```
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

Esempi: Registrazione degli eventi di rete per i datastore di eventi

È possibile configurare i datastore di eventi per includere eventi di attività di rete utilizzando la AWS CLI. Utilizza il `create-event-data-store`comando per creare un nuovo datastore di eventi per registrare gli eventi di attività di rete. Utilizza il comando `update-event-data-store` per aggiornare i selettori di eventi avanzati per un datastore di eventi esistente.

Per verificare se il datastore di eventi include eventi di rete, esegui il `get-event-data-store`comando.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

Argomenti

- Esempio: registra tutti gli eventi di attività di rete per CloudTrail le operazioni
- Esempio: registra VpceAccessDenied gli eventi per AWS KMS
- Esempio: registra EC2 VpceAccessDenied gli eventi su un endpoint VPC specifico
- Esempio: Registrazione di VpceAccessDenied eventi di registrazione per Amazon S3
- Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi

Esempio: registra tutti gli eventi di attività di rete per CloudTrail le operazioni

Nell'esempio seguente viene illustrato come creare un datastore di eventi che include tutti gli eventi di rete correlati alle CloudTrail operazioni, ad esempio le chiamate a `CreateTrail` e`CreateEventDataStore`. Il valore del `eventSource` campo è impostato su`cloudtrail.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name "EventDataStoreName" \
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls over VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit all CloudTrail API calls over VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Esempio: registra **`VpceAccessDenied`** gli eventi per AWS KMS

Nell'esempio seguente viene illustrato come creare un datastore di eventi per includere `VpceAccessDenied` eventi di eventi AWS KMS. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi e il `eventSource` campo uguale a`kms.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
```

```
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Esempio: registra EC2 **`VpceAccessDenied`** gli eventi su un endpoint VPC specifico

L'esempio seguente mostra come creare un datastore di eventi per includere `VpceAccessDenied` eventi per Amazon EC2 per un endpoint VPC specifico. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi, il `eventSource` campo uguale e `vpcEndpointId` uguale all'endpoint VPC di interesse. `ec2.amazonaws.com`

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Esempio: Registrazione di **`VpceAccessDenied`** eventi di registrazione per Amazon S3

L'esempio seguente mostra come creare un datastore di eventi per includere `VpceAccessDenied` eventi per Amazon S3. Questo esempio imposta il `errorCode` campo uguale agli `VpceAccessDenied` eventi e il `eventSource` campo uguale a`s3.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
```

```
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
```

```
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
     ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Esempio: registra tutti gli eventi di gestione e gli eventi di attività di rete per più fonti di eventi

Gli esempi seguenti aggiornano un archivio dati di eventi che attualmente registra solo gli eventi di gestione per registrare anche gli eventi di attività di rete per più fonti di eventi. Per aggiornare un archivio dati di eventi per aggiungere nuovi selettori di eventi, esegui il `get-event-data-store` comando per restituire i selettori di eventi avanzati correnti. Quindi, esegui il `update-event-data-store` comando e passa `--advanced-event-selectors` quello che include i selettori correnti più eventuali nuovi selettori. Per registrare gli eventi di attività di rete per più fonti di eventi, includi un selettore per ogni fonte di eventi che desideri registrare.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
```

```
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]},
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
```

```
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

Questo comando restituisce il seguente output di esempio.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
           {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
```

```
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
```

```
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-20T21:00:17.673000+00:00",
```

```
    "UpdatedTimestamp": "2024-11-20T21:00:17.820000+00:00"
}
```

Registrazione degli eventi con AWS SDKs

Esegui l'GetEventSelectorsoperazione per verificare se il percorso sta registrando eventi di attività di rete. Puoi configurare i percorsi per la registrazione di eventi di rete eseguendo l'PutEventSelectorsoperazione. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS CloudTrail.

Esegui l'GetEventDataStoreoperazione per verificare se il datastore di eventi sta registrando gli eventi di rete. È possibile configurare i data store degli eventi per includere gli eventi di attività di rete eseguendo UpdateEventDataStorele operazioni CreateEventDataStoreor e specificando selettori di eventi avanzati. Per ulteriori informazioni, consulta Crea, aggiorna e gestisci gli archivi dati degli eventi con AWS CLI e il Riferimento API di AWS CloudTrail.

Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM

Puoi arricchire gli eventi di CloudTrail gestione e gli eventi relativi ai dati aggiungendo chiavi di tag di risorsa, chiavi di tag principali e chiavi di condizione globale IAM quando crei o aggiorni un data store di eventi. Ciò consente di classificare, cercare e analizzare CloudTrail gli eventi in base al contesto aziendale, come l'allocazione dei costi e la gestione finanziaria, le operazioni e i requisiti di sicurezza dei dati. Puoi analizzare gli eventi eseguendo query in Lake. CloudTrail Puoi anche scegliere di federare il tuo archivio dati di eventi ed eseguire query in Amazon Athena. Puoi aggiungere chiavi di tag di risorsa e chiavi di condizione globali IAM a un data store di eventi utilizzando la CloudTrail console e. AWS CLI SDKs

> **Note**
>
> I tag delle risorse che aggiungi dopo la creazione o gli aggiornamenti delle risorse potrebbero subire un ritardo prima che tali tag si riflettano negli CloudTrail eventi. CloudTrail gli eventi per l'eliminazione delle risorse potrebbero non includere informazioni sui tag.
> Le chiavi delle condizioni globali IAM saranno sempre visibili nell'output di una query, ma potrebbero non essere visibili al proprietario della risorsa.

Quando aggiungi chiavi di tag di risorsa a eventi arricchiti, CloudTrail include le chiavi tag selezionate associate alle risorse coinvolte nella chiamata API.

Quando aggiungi chiavi di condizione globali IAM a un archivio dati di eventi, CloudTrail include informazioni sulle chiavi di condizione selezionate che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione e sulla richiesta stessa.

> **Note**
>
> La configurazione CloudTrail per includere una chiave di condizione o un tag principale non significa che tale chiave di condizione o tag principale sarà presente in ogni evento. Ad esempio, se hai impostato l'inclusione CloudTrail di una chiave di condizione globale specifica ma non la vedi in un evento particolare, ciò indica che la chiave non era rilevante per la valutazione della policy IAM relativa a quell'azione.

Dopo aver aggiunto le chiavi dei tag di risorsa o le chiavi di condizione IAM, CloudTrail include un `eventContext` campo negli CloudTrail eventi che fornisce le informazioni contestuali selezionate per l'azione dell'API.

Esistono alcune eccezioni quando l'evento non includerà il `eventContext` campo, tra cui:

- Gli eventi API relativi alle risorse eliminate potrebbero avere o meno tag di risorsa.
- Il `eventContext` campo non conterrà dati sugli eventi ritardati e non sarà presente per gli eventi che sono stati aggiornati dopo la chiamata API. Ad esempio, se si verifica un ritardo o un'interruzione per Amazon EventBridge, i tag per gli eventi potrebbero rimanere obsoleti per qualche tempo dopo la risoluzione dell'interruzione. Alcuni AWS servizi subiranno ritardi più lunghi. Per ulteriori informazioni, consulta Aggiornamenti dei tag di risorsa CloudTrail per eventi arricchiti.
- Se modifichi o elimini il ruolo AWSService RoleForCloudTrailEventContext collegato al servizio utilizzato per gli eventi arricchiti, non CloudTrail inserirà alcun tag di risorsa in. `eventContext`

> **Note**
>
> Il `eventContext` campo è presente solo negli eventi per gli archivi di dati di eventi configurati per includere chiavi di tag di risorsa, chiavi di tag principali e chiavi di condizione globali IAM. Gli eventi inviati a Event history, Amazon EventBridge, visualizzabili con il AWS

CLI `lookup-events` comando e consegnati ai trail, non includeranno il `eventContext` campo.

Argomenti

- Servizi AWS tag di risorse di supporto
- Servizi AWS supporto delle chiavi di condizione globali IAM
- Esempi di eventi

Servizi AWS tag di risorse di supporto

Tutti i tag delle risorse di Servizi AWS supporto. Per ulteriori informazioni, consulta Servizi che supportano il AWS Resource Groups Tagging API.

Aggiornamenti dei tag di risorsa CloudTrail per eventi arricchiti

Se configurato per farlo, CloudTrail acquisisce informazioni sui tag delle risorse e le utilizza per fornire informazioni negli eventi arricchiti. Quando si lavora con i tag di risorsa, ci sono alcune condizioni in cui un tag di risorsa potrebbe non essere riflesso accuratamente al momento della richiesta di eventi del sistema. Durante il funzionamento standard, i tag applicati al momento della creazione delle risorse sono sempre presenti e subiranno ritardi minimi o nulli. Tuttavia, si prevede che i seguenti servizi presentino ritardi nella visualizzazione delle modifiche ai tag delle risorse negli eventi: CloudTrail

- Connettore voce Amazon Chime
- AWS CloudTrail
- AWS CodeConnections
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Keyspaces (per Apache Cassandra)
- Amazon Kinesis
- Amazon Lex
- Amazon MemoryDB
- Amazon S3

- Amazon Security Lake
- AWS Direct Connect
- AWS IAM Identity Center
- AWS Key Management Service
- AWS Lambda
- Marketplace AWS Vendor Insights
- AWS Organizations
- AWS Payment Cryptography
- Amazon Simple Queue Service

Le interruzioni del servizio possono anche causare ritardi negli aggiornamenti delle informazioni sui tag delle risorse. In caso di ritardo nell'interruzione del servizio, CloudTrail gli eventi successivi includeranno un `addendum` campo che include informazioni sulla modifica del tag di risorsa. Queste informazioni aggiuntive verranno utilizzate come specificato per fornire informazioni arricchiteCloudTrailevents.

Servizi AWS supporto delle chiavi di condizione globali IAM

Quanto segue Servizi AWS supporta le chiavi di condizione globali IAM per eventi arricchiti:

- AWS Certificate Manager
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Registri Amazon
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon Cognito Sync
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect Voice ID
- AWS Control Tower
- Amazon Data Firehose

- Amazon Elastic Block Store
- Sistema di bilanciamento del carico elastico
- AWS End User Messaging Social
- Amazon EventBridge
- Amazon EventBridge Scheduler
- Amazon Data Firehose
- Amazon FSx
- AWS HealthImaging
- AWS IoT Events
- AWS IoT FleetWise
- AWS IoT SiteWise
- AWS IoT TwinMaker
- Wireless AWS IoT
- Amazon Kendra
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Lookout per le apparecchiature
- Amazon Lookout per Vision
- AWS Network Firewall
- AWS Payment Cryptography
- Amazon Personalize
- AWS Proton
- Amazon Rekognition
- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Email Service (Amazon SES)
- Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))
- Amazon SQS
- AWS Step Functions

- AWS Storage Gateway
- Amazon SWF
- Catena di approvvigionamento di AWS
- Amazon Timestream
- Amazon Timestream per InfluxDB
- Amazon Transcribe
- AWS Transfer Family
- AWS Trusted Advisor
- Amazon WorkSpaces
- AWS X-Ray

Chiavi di condizione globali IAM supportate per eventi arricchiti

La tabella seguente elenca le chiavi di condizione globali IAM supportate per eventi CloudTrail arricchiti, con valori di esempio:

Chiavi della condizione globale e valori di esempio

Chiave	Valore di esempio
`aws:FederatedProvider`	"*IdP*"
`aws:TokenIssueTime`	"*123456789* "
`aws:MultiFactorAuthAge`	«99"
`aws:MultiFactorAuthPresent`	"*true*"
`aws:SourceIdentity`	"*UserName*"
`aws:PrincipalAccount`	«111122223333"
`aws:PrincipalArn`	«arn:aws:iam::» *555555555555:role/myRole*
`aws:PrincipalIsAWSService`	"*false*"
`aws:PrincipalOrgI D`	"*o-rganization* "

Chiave	Valore di esempio
aws:PrincipalOrgPaths	["o-rganization/path-of-org "]
aws:PrincipalServiceName	"cloudtrail.amazonaws.com "
aws:PrincipalServiceNamesList	["cloudtrail.amazonaws.com"," s3.amazonaws.com "]
aws:PrincipalType	"AssumedRole "
aws:userid	"userid"
aws:username	"username"
aws:RequestedRegion	us-east-2 "
aws:SecureTransport	"true"
aws:ViaAWSService	"false"
aws:CurrentTime	"2025-04-30 15:30:00 "
aws:EpochTime	"1746049800 "
aws:SourceAccount	"111111111111 "
aws:SourceOrgID	"o-rganization "

Esempi di eventi

Nell'esempio seguente, il `eventContext` campo include una chiave di condizione globale IAM `aws:ViaAWSService` con un valore di`false`, che indica che la chiamata API non è stata effettuata da un. Servizio AWS

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/admin",
```

```
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/admin",
                "accountId": "123456789012",
                "userName": "admin"
            },
            "attributes": {
                "creationDate": "2025-01-22T22:05:56Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-01-22T22:06:16Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "GetTrailStatus",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:133.0)
 Gecko/20100101 Firefox/133.0",
    "requestParameters": {
        "name": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail"
    },
    "responseElements": null,
    "requestID": "d09c4dd2-5698-412b-be7a-example1a23",
    "eventID": "9cb5f426-7806-46e5-9729-exampled135d",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true",
    "eventContext": {
        "requestContext": {
            "aws:ViaAWSService": "false"
        },
```

```
        "tagContext": {}
    }
}
```

CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete

Questa pagina descrive il contenuto dei record di un evento di gestione, dati o attività di rete.

Il corpo del record contiene i campi che consentono di determinare l'azione richiesta, nonché quando e dove la richiesta è stata effettuata. Quando il valore di Optional è True, il campo è presente solo quando si applica al servizio, all'API o al tipo di evento. Un valore Optional (Facoltativo) di False indica che il campo è sempre presente o che la sua presenza non dipende dal servizio, dall'API o dal tipo di evento. Un esempio è `responseElements`, presente negli eventi per operazioni che comportano modifiche (operazioni di creazione, aggiornamento o eliminazione).

> **Note**
>
> I campi per eventi arricchiti, ad esempio, `eventContext` sono disponibili solo per gli eventi di gestione e gli eventi relativi ai dati. Non sono disponibili per gli eventi di rete.

`eventTime`

Data e ora in cui è stata completata la richiesta in formato UTC (Coordinated Universal Time). La marca temporale di un evento proviene dall'host locale che fornisce l'endpoint API del servizio su cui è stata effettuata la chiamata API. Ad esempio, un evento CreateBucket API eseguito nella regione Stati Uniti occidentali (Oregon) ottiene la relativa marca temporale dall'ora di un AWS host che esegue l'endpoint Amazon S3. `s3.us-west-2.amazonaws.com` In generale, AWS i servizi utilizzano NTP (Network Time Protocol) per sincronizzare gli orologi di sistema.

Since: 1.0

Optional: False

`eventVersion`

Versione del formato dell'evento di log. La versione corrente è 1.11.

Il `eventVersion` valore è una versione maggiore e minore nel formato*`major_version`*. *`minor_version`*. Ad esempio, puoi avere un valore `eventVersion` di `1.10`, dove 1 è la versione principale e `10` è la versione secondaria.

CloudTrail incrementa la versione principale se viene apportata una modifica alla struttura dell'evento che non è compatibile con le versioni precedenti. Questo include la rimozione di un campo JSON che esiste già o la modifica del modo in cui i contenuti di un campo sono rappresentati (ad esempio, un formato di data). CloudTrail incrementa la versione secondaria se una modifica aggiunge nuovi campi alla struttura dell'evento. Questo può verificarsi se sono disponibili nuove informazioni per alcuni o tutti gli eventi esistenti oppure se sono disponibili nuove informazioni solo per novi tipi di eventi. Le applicazioni possono ignorare i nuovi campi per rimanere compatibili con le nuove versioni secondarie della struttura dell'evento.

Se CloudTrail introduce nuovi tipi di eventi, ma la struttura dell'evento rimane invariata, la versione dell'evento non cambia.

Per essere certi che le applicazioni possano analizzare la struttura dell'evento, è consigliabile eseguire un confronto "uguale a" sul numero della versione principale. Per essere certi che i campi richiesti dall'applicazione siano presenti, è inoltre consigliabile eseguire un confronto greater-than-or-equal -to sulla versione secondaria. Non sono presenti zeri iniziali nella versione secondaria. Puoi interpretare entrambi *`major_version`* e *`minor_version`* come numeri ed eseguire operazioni di confronto.

Since: 1.0

Optional: False

`userIdentity`

Informazioni relative all'identità IAM che ha effettuato una richiesta. Per ulteriori informazioni, consulta CloudTrail elemento userIdentity.

Since: 1.0

Optional: False

`eventSource`

Servizio a cui è stata eseguita la richiesta. Questo nome è in genere la versione abbreviata del nome del servizio senza spazi e con il suffisso `.amazonaws.com`. Per esempio:

- AWS CloudFormation è`cloudformation.amazonaws.com`.

- Amazon EC2 lo è`ec2.amazonaws.com`.
- Amazon Simple Workflow Service è `swf.amazonaws.com`.

Questa convenzione è caratterizzata da alcune eccezioni. Ad esempio, `eventSource` per Amazon CloudWatch è`monitoring.amazonaws.com`.

Since: 1.0

Optional: False

`eventName`

Operazione richiesta, che è una delle operazioni nell'API per il servizio specifico.

Since: 1.0

Optional: False

`awsRegion`

Il Regione AWS destinatario della richiesta, ad esempio`us-east-2`. Consultare CloudTrail Regioni supportate.

Since: 1.0

Optional: False

`sourceIPAddress`

Indirizzo IP da cui è stata effettuata la richiesta. Per le operazioni che hanno origine dalla console del servizio, l'indirizzo rilevato fa riferimento alla risorsa cliente sottostante, non al server Web della console. Per i servizi in AWS, viene visualizzato solo il nome DNS.

> **Note**
>
> Per gli eventi generati da AWS, questo campo è in genere `AWS Internal/#`, dove `#` rappresenta un numero utilizzato per scopi interni.

Since: 1.0

Optional: False

`userAgent`

L'agente tramite il quale è stata effettuata la richiesta, ad esempio il AWS Management Console, un AWS servizio, il AWS SDKs o il AWS CLI.

Questo campo ha una dimensione massima di 1 KB. Il contenuto che supera tale limite viene troncato. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene troncato solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Di seguito sono riportati i valori di esempio:

- `lambda.amazonaws.com` - La richiesta è stata effettuata con AWS Lambda.
- `aws-sdk-java` - La richiesta è stata effettuata con AWS SDK per Java.
- `aws-sdk-ruby` - La richiesta è stata effettuata con AWS SDK per Ruby.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— La richiesta è stata effettuata con l'installazione su Linux. AWS CLI

> **Note**
>
> Per gli eventi generati da AWS, se CloudTrail sa chi Servizio AWS ha effettuato la chiamata, questo campo è l'origine dell'evento del servizio chiamante (ad esempio,`ec2.amazonaws.com`). Altrimenti, questo campo è `AWS Internal/#` dove si `#` trova un numero utilizzato per scopi interni.

Since: 1.0

Optional: True

`errorCode`

L'errore di AWS servizio se la richiesta restituisce un errore. Per un esempio che mostra questo campo, consulta Esempio di codice di errore e log dei messaggi.

Questo campo ha una dimensione massima di 1 KB. Il contenuto che supera tale limite viene troncato. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il

contenuto del campo viene troncato solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Per gli eventi di attività di rete, in caso di violazione delle policy degli endpoint VPC, il codice di errore è. `VpceAccessDenied`

Since: 1.0

Optional: True

`errorMessage`

Descrizione dell'errore, se la richiesta restituisce un errore. Questo messaggio include messaggi relativi agli errori di autorizzazione. CloudTrail acquisisce il messaggio registrato dal servizio durante la relativa gestione delle eccezioni. Per vedere un esempio, consulta Esempio di codice di errore e log dei messaggi.

Questo campo ha una dimensione massima di 1 KB. Il contenuto che supera tale limite viene troncato. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene troncato solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Per gli eventi di attività di rete, in caso di violazione della policy degli endpoint VPC, `errorMessage` verrà sempre visualizzato il seguente messaggio:. `The request was denied due to a VPC endpoint policy` Per ulteriori informazioni sugli eventi di accesso negato per le violazioni delle policy degli endpoint VPC, consulta Esempi di messaggi di errore di accesso negato nella IAM User Guide. Per un esempio di evento di attività di rete che mostra una violazione delle policy degli endpoint VPC, consulta Eventi di attività di rete in questa guida.

> **Note**
>
> Alcuni AWS servizi forniscono gli `errorCode` e `errorMessage` come campi di primo livello nell'evento. Altri servizi AWS restituiscono informazioni di errore come parte di `responseElements`.

Since: 1.0

Optional: True

`requestParameters`

Eventuali parametri stati inviati assieme alla richiesta. Questi parametri sono documentati nella documentazione di riferimento dell'API per il servizio appropriato AWS . Questo campo ha una dimensione massima di 100 KB. Quando la dimensione del campo supera i 100 KB, il `requestParameters` contenuto viene omesso. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene omesso solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Since: 1.0

Optional: False

`responseElements`

Gli elementi di risposta, se presenti, per operazioni che comportano modifiche (operazioni di creazione, aggiornamento o eliminazione). Per `readOnly` APIs, questo campo è`null`. Se l'azione non restituisce elementi di risposta, questo campo è`null`. Gli elementi di risposta per le azioni sono documentati nel riferimento all'API documentazione appropriata Servizio AWS.

Questo campo ha una dimensione massima di 100 KB. Quando la dimensione del campo supera i 100 KB, il `reponseElements` contenuto viene omesso. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene omesso solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Il `responseElements` valore è utile per aiutarti a tracciare una richiesta. con Supporto AWS. Entrambi `x-amz-request-id` e `x-amz-id-2` contengono informazioni che consentono di tracciare una richiesta con Supporto. Questi valori sono gli stessi che il servizio restituisce nella risposta alla richiesta che avvia gli eventi, in modo che sia possibile utilizzarli per abbinare l'evento a una richiesta.

Since: 1.0

Optional: False

`additionalEventData`

Dati aggiuntivi sull'evento non facenti parte della richiesta o della risposta. Questo campo ha una dimensione massima di 28 KB. Quando la dimensione del campo supera i 28 KB, il

`additionalEventData` contenuto viene omesso. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene omesso solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Il contenuto di è variabile. `additionalEventData` Ad esempio, per gli eventi di AWS Management Console accesso, `additionalEventData` potrebbe includere il `MFAUsed` campo con il valore `Yes` se la richiesta è stata effettuata da un utente root o IAM utilizzando l'autenticazione a più fattori (MFA).

Since: 1.0

Optional: True

`requestID`

Valore che identifica la richiesta. Il servizio chiamato genera questo valore. Questo campo ha una dimensione massima di 1 KB. Il contenuto che supera tale limite viene troncato. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene troncato solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Since: 1.01

Optional: True

`eventID`

GUID generato da CloudTrail per identificare in modo univoco ogni evento. Puoi utilizzare questo valore per identificare un singolo evento. Ad esempio, puoi utilizzare l'ID come chiave primaria per recuperare i dati di log da un database ricercabile.

Since: 1.01

Optional: False

`eventType`

Identifica il tipo di evento che ha generato il record dell'evento. Può essere uno dei seguenti valori:

- `AwsApiCall` - Un'API è stata chiamata.

- `AwsServiceEvent` - Il servizio ha generato un evento correlato al percorso. Ad esempio, ciò si può verificare quando un altro account ha effettuato una chiamata con una risorsa di tua proprietà.
- `AwsConsoleAction` - Nella console è stata eseguita un'azione che non era una chiamata API.
- `AwsConsoleSignIn`— Un utente del tuo account (root, IAM, federated, SAML o SwitchRole) ha effettuato l'accesso a. AWS Management Console
- `AwsVpceEvents`— gli eventi di attività di CloudTrail rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Per registrare gli eventi di attività di rete, il proprietario dell'endpoint VPC deve abilitare gli eventi di attività di rete per l'origine dell'evento.

Since: 1.02

Optional: False

`apiVersion`

Identifica la versione API associata al valore `AwsApiCall` `eventType`.

Since: 1.01

Optional: True

`managementEvent`

Un valore booleano che identifica se l'evento è un evento di gestione. `managementEvent` viene mostrato in un record di eventi se `eventVersion` è 1.06 o superiore e il tipo di evento è uno dei seguenti:

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Since: 1.06

Optional: True

`readOnly`

Identifica se questa operazione è un'operazione di sola lettura. Può essere uno dei seguenti valori:

- `true` - L'operazione è di sola lettura (ad esempio, `DescribeTrails`).
- `false` - L'operazione è di sola scrittura (ad esempio, `DeleteTrail`).

Since: 1.01

Optional: True

`resources`

Elenco delle risorse a cui è stato eseguito l'accesso nell'evento. Il campo può contenere le informazioni seguenti:

- Risorsa ARNs
- ID account del proprietario delle risorse
- Identificatore del tipo di risorsa nel formato: `AWS::`*`aws-service-name`*`::`*`data-type-name`*

Ad esempio, quando viene registrato un evento `AssumeRole`, il campo `resources` può avere il seguente aspetto:

- ARN: `arn:aws:iam::123456789012:role/`*`myRole`*
- ID account: `123456789012`
- Identificatore del tipo di risorsa: `AWS::IAM::Role`

Ad esempio, i log con il `resources` campo, consulta AWS STS API Event in CloudTrail Log File nella IAM User Guide o Logging AWS KMS API Calls nella AWS Key Management Service Developer Guide.

Since: 1.01

Optional: True

`recipientAccountId`

Rappresenta l'ID dell'account che ha ricevuto questo evento. `recipientAccountID` può essere diverso da CloudTrail elemento userIdentity `accountId`. Questo può verificarsi nell'accesso alle risorse da più account. Ad esempio, se una chiave KMS, definita anche AWS KMS key,

è stata utilizzata da un account diverso per chiamare l'API di crittografia, i valori `accountId` e `recipientAccountID` sono uguali per l'evento distribuito all'account che ha effettuato la chiamata, ma sono diversi per l'evento distribuito all'account proprietario della chiave KMS.

Since: 1.02

Optional: True

`serviceEventDetails`

Identifica l'evento del servizio, incluso l'elemento che ha attivato l'evento e il risultato. Per ulteriori informazioni, consulta Servizio AWS eventi. Questo campo ha una dimensione massima di 100 KB. Quando la dimensione del campo supera i 100 KB, il `serviceEventDetails` contenuto viene omesso. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene omesso solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Since: 1.05

Optional: True

`sharedEventID`

GUID generato da CloudTrail per identificare in modo univoco CloudTrail gli eventi derivanti dalla stessa AWS operazione inviata a diversi AWS account.

Ad esempio, quando un account utilizza una AWS KMS keyappartenente a un altro account, l'account che ha utilizzato la chiave KMS e l'account proprietario della chiave KMS ricevono CloudTrail eventi separati per la stessa operazione. Ogni CloudTrail evento fornito per questa AWS azione è lo stesso`sharedEventID`, ma ha anche un unico `eventID` e. `recipientAccountID`

Per ulteriori informazioni, consulta Esempio di sharedEventID.

> **Note**
>
> Il `sharedEventID` campo è presente solo quando CloudTrail gli eventi vengono distribuiti su più account. Se l'autore della chiamata e il proprietario sono lo stesso account AWS , CloudTrail invia solo un evento e il campo `sharedEventID` non è presente.

Since: 1.03

Optional: True

`vpcEndpointId`

Identifica l'endpoint VPC in cui le richieste sono state effettuate da un VPC a un altro AWS servizio, ad esempio Amazon. EC2

> **Note**
>
> Per gli eventi generati da AWS e tramite il VPC Servizio AWS di un utente, questo campo è in `AWS Internal` genere o il nome del servizio.

Since: 1.04

Optional: True

`vpcEndpointAccountId`

Identifica l' Account AWS ID del proprietario dell'endpoint VPC per l'endpoint corrispondente per il quale è stata inoltrata una richiesta.

> **Note**
>
> Per gli eventi generati da AWS e tramite il VPC Servizio AWS di un utente, questo campo è in `AWS Internal` genere o il nome del servizio.

Dal: 1.09

Optional: True

`eventCategory`

Mostra la categoria dell'evento. La categoria di eventi viene utilizzata nelle `LookupEvents`chiamate per filtrare gli eventi di gestione.

- Per gli eventi di gestione, il valore è `Management`.
- Per gli eventi di dati, il valore è `Data`.
- Per gli eventi di attività di rete, il valore è`NetworkActivity`.

Since: 1.07

Optional: False

`addendum`

Se la consegna di un evento ha subito un ritardo o se diventano disponibili ulteriori informazioni su un evento esistente dopo la registrazione dell'evento, un campo addendum mostra informazioni sul motivo per cui l'evento ha subito un ritardo. Se mancavano informazioni da un evento esistente, il campo addendum include le informazioni mancanti e un motivo per cui mancavano. Il contenuto include quanto segue.

- **`reason`** - Il motivo per cui l'evento o alcuni dei suoi contenuti mancavano. I valori possono essere uno dei seguenti.
  - **`DELIVERY_DELAY`** - La consegna degli eventi ha subito un ritardo. Ciò potrebbe essere causato da un elevato traffico di rete, problemi di connettività o un problema CloudTrail di servizio.
  - **`UPDATED_DATA`** - Un campo nel record dell'evento mancava o aveva un valore non corretto.
  - **`SERVICE_OUTAGE`**— Un servizio che registra gli eventi CloudTrail ha avuto un'interruzione e in cui non ha potuto registrare gli eventi. CloudTrail Questo è eccezionalmente raro.
- **`updatedFields`** - I campi record di evento aggiornati dall'addendum. Questo è fornito solo se il motivo è `UPDATED_DATA`.
- **`originalRequestID`** - L'ID univoco originale della richiesta. Questo è fornito solo se il motivo è `UPDATED_DATA`.
- **`originalEventID`** - L'ID evento originale. Questo è fornito solo se il motivo è `UPDATED_DATA`.

Since: 1.08

Optional: True

`sessionCredentialFromConsole`

Stringa con un valore di `true` o `false` che mostra se un evento ha avuto origine da una AWS Management Console sessione. Questo campo non viene visualizzato a meno che il valore

sia `true`, che indica che il client utilizzato per effettuare la chiamata API era un proxy o un client esterno. Se è stato utilizzato un client proxy, il campo dell'evento `tlsDetails` non viene visualizzato.

Since: 1.08

Optional: True

`eventContext`

Questo campo è presente negli eventi arricchiti registrati per gli archivi di dati di eventi che sono stati configurati per includere chiavi di tag di risorsa o chiavi di condizione globali IAM. Per ulteriori informazioni, consulta Arricchisci CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.

Il contenuto include quanto segue:

- `requestContext`— Include informazioni sulle chiavi delle condizioni globali IAM che sono state valutate durante il processo di autorizzazione, inclusi dettagli aggiuntivi sul principale, sulla sessione, sulla rete e sulla richiesta stessa.
- `tagContext`— Include i tag associati alle risorse coinvolte nella chiamata API e i tag associati ai principali IAM come ruoli o utenti. Per ulteriori informazioni, consulta Controllo dell'accesso per i principali di IAM.

  Gli eventi API relativi alle risorse eliminate non avranno tag di risorsa.

> **Note**
>
> Il `eventContext` campo è presente solo negli eventi per gli archivi di dati di eventi configurati per includere chiavi di tag di risorsa e chiavi di condizione globali IAM. Gli eventi inviati a Event history, Amazon EventBridge, visualizzabili con il AWS CLI `lookup-events` comando e consegnati ai trail, non includeranno il `eventContext` campo.

Dal: 1.11

Optional: True

`edgeDeviceDetails`

Mostra informazioni sui dispositivi edge che sono destinazioni di una richiesta. Attualmente, gli eventi dei dispositivi `S3 Outposts` includono questo campo. Questo campo ha una dimensione

massima di 28 KB. Il contenuto che supera tale limite viene troncato. Per gli archivi dati di eventi configurati per avere una dimensione massima di 1 MB, il contenuto del campo viene troncato solo se il payload dell'evento supera 1 MB e viene superata la dimensione massima del campo.

Since: 1.08

Optional: True

`tlsDetails`

Mostra informazioni sulla versione di Transport Layer Security (TLS), le suite di crittografia e il nome dominio completo del nome host fornito dal client utilizzato nella chiamata API di servizio, che di solito è il nome dominio completo dell'endpoint di servizio. CloudTrailregistra ancora i dettagli TLS parziali se le informazioni previste sono mancanti o vuote. Ad esempio, se la versione TLS e la suite di crittografia sono presenti, ma l'`HOST`intestazione è vuota, i dettagli TLS disponibili vengono ancora registrati nell'evento. CloudTrail

- **`tlsVersion`** - La versione TLS di una richiesta.
- **`cipherSuite`** - La suite di crittografia (combinazione di algoritmi di sicurezza utilizzati) di una richiesta.
- **`clientProvidedHostHeader`**: il nome host fornito dal client utilizzato nella chiamata API del servizio, che in genere è il nome di dominio completo dell'endpoint del servizio.

> **Note**
>
> In alcuni casi il campo `tlsDetails` non è presente in un record di eventi.
>
> - Il `tlsDetails` campo non è presente se la chiamata API è stata effettuata da un per tuo Servizio AWS conto. Il campo `invokedBy` nell'elemento `userIdentity` identifica il Servizio AWS che ha effettuato la chiamata API.
> - Se `sessionCredentialFromConsole` è presente con un valore true, `tlsDetails` è presente in un record di eventi solo se per effettuare la chiamata API è stato utilizzato un client esterno.

Since: 1.08

Optional: True

Ordine di troncamento dei campi per una dimensione massima dell'evento di 1 MB

È possibile espandere la dimensione massima dell'evento da 256 KB a 1 MB quando si crea o si aggiorna un archivio dati di eventi utilizzando la CloudTrail console e. AWS CLI SDKs

L'espansione della dimensione dell'evento è utile per l'analisi e la risoluzione dei problemi degli eventi, poiché consente di visualizzare il contenuto completo dei campi che normalmente verrebbero troncati o omessi.

Quando il payload dell'evento supera 1 MB, CloudTrail tronca i campi nel seguente ordine:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `eventContext`
- `responseElements`
- `requestParameters`
- `errorMessage`

Se il payload di un evento non può essere ridotto a meno di 1 MB anche dopo il troncamento, si verificherà un errore.

Esempio di sharedEventID

Di seguito è riportato un esempio che descrive come CloudTrail distribuisce due eventi per la stessa operazione:

1. Alice dispone di un AWS account (1111) e crea un' AWS KMS key. È proprietaria di questa chiave KMS.
2. Bob dispone di un AWS account (222222222222). Alice concede a Bob l'autorizzazione per utilizzare la chiave KMS.
3. Ogni account dispone di un trail e di un bucket distinto.

4. Bob usa la chiave KMS per chiamare l'API `Encrypt`.
5. CloudTrail invia due eventi separati.
   - Un evento viene inviato a Bob. L'evento mostra che ha utilizzato la chiave KMS.
   - Un evento viene inviato ad Alice. L'evento mostra che Bob ha utilizzato la chiave KMS.
   - Gli eventi hanno lo stesso valore di `sharedEventID`, ma i valori `eventID` e `recipientAccountID` sono univoci.

CloudTrail registra contenuti per gli eventi Insights per i percorsi

AWS CloudTrail I record degli eventi Insights per i percorsi includono campi diversi da altri CloudTrail eventi nella loro struttura JSON, a volte chiamati payload. CloudTrail Gli eventi Insights per i trail contengono i seguenti campi:

- **`eventVersion`**— La versione dell'evento.

  Since: 1.07

  Optional: False
- **`eventType`**— Il tipo di evento. Il valore è sempre `AwsCloudTrailInsight` per gli eventi Insights.

  Since: 1.07

  Optional: False
- **`eventID`**: GUID generato da CloudTrail per identificare in modo univoco ogni evento. Puoi utilizzare questo valore per identificare un singolo evento. Ad esempio, puoi utilizzare l'ID come chiave primaria per recuperare i dati di log da un database ricercabile.

  Since: 1.07

  Optional: False
- **`eventTime`**: l'ora di inizio o di fine dell'evento Insights, espressa nel Tempo coordinato universale (UTC).

  Since: 1.07

Optional: False

- **`awsRegion`**— Il Regione AWS luogo in cui si è verificato l'evento Insights, ad esempio`us-east-2`.

  Since: 1.07

  Optional: False

- **`recipientAccountId`**: rappresenta l'ID dell'account che ha ricevuto questo evento.

  Since: 1.07

  Optional: True

- **`sharedEventID`**— Un GUID generato da CloudTrail Insights per identificare in modo univoco un evento Insights. `sharedEventID`è comune tra gli eventi Insights di inizio e di fine e consente di connettere entrambi gli eventi per identificare in modo univoco l'attività insolita. Puoi considerare lo `sharedEventID` come l'ID evento generale di Insights.

  Since: 1.07

  Optional: False

- **`insightDetails`**: un record di eventi CloudTrail Insights per un percorso include un *`insightDetails`* blocco che contiene informazioni sui trigger sottostanti di un evento Insights, ad esempio origine evento, identità utente, agenti dell'utente, medie cronologiche o riferimenti, statistiche, nome dell'API e se l'evento è quello di inizio o di fine dell'evento Insights.

  Since: 1.07

  Optional: False

  - **`state`**: indica se l'evento è l'evento Insights di inizio o di fine. Il valore può essere `Start` o `End`.

    Since: 1.07

    Optional: False

  - **`eventSource`**— Il AWS servizio all'origine dell'attività insolita, ad esempio`ec2.amazonaws.com`.

    Since: 1.07

    Optional: False

- **`eventName`**: il nome dell'evento Insights, in genere il nome dell'API che ha dato origine all'attività insolita.

  Since: 1.07

  Optional: False

- **`insightType`**— Il tipo di evento Insights. Questo valore può essere `ApiCallRateInsight` o `ApiErrorRateInsight`.

  Since: 1.07

  Optional: False

- **`errorCode`**— Il codice di errore dell'attività insolita. Consulta anche `errorCode` in CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

  Since: 1.07

  Optional: True

- **`insightContext`**— Informazioni su AWS strumenti (chiamati agenti dell'utente), utenti e ruoli IAM (chiamati identità utente) e codici di errore associati agli eventi CloudTrail analizzati per generare l'evento Insights. Questo elemento include anche statistiche che mostrano il modo in cui l'attività insolita in un evento Insights viene confrontata con l'attività di riferimento o normale.

  Since: 1.07

  Optional: False

  - **`statistics`**: include i dati relativi al riferimento, o frequenza media tipica delle chiamate o degli errori all'API oggetto da parte di un account, misurata durante il periodo di base, la frequenza media delle chiamate o degli errori che hanno attivato l'evento Insights, la durata, espressa in minuti, dell'evento Insights e la durata, espressa in minuti, del periodo di misurazione di base.

    Since: 1.07

    Optional: False

    - **`baseline`**: le chiamate o gli errori API al minuto per la durata di riferimento all'API oggetto dell'evento Insights per l'account, calcolata nei sette giorni precedenti all'inizio dell'evento Insights.

Since: 1.07

Optional: False

- **`average`**: la media cronologica delle chiamate o degli errori API al minuto durante i sette giorni precedenti all'ora di inizio dell'attività Insights.

  Since: 1.07

  Optional: False

- **`insight`**: per un evento Insights di inizio, questo valore è il numero medio di chiamate o errori API al minuto durante l'inizio dell'attività insolita. Per un evento Insights di fine, questo valore è il numero medio di chiamate o erriri API al minuto per la durata dell'attività insolita.

  Since: 1.07

  Optional: False

  - **`average`**: il numero medio di chiamate o errori API registrati al minuto durante il periodo di attività insolita.

    Since: 1.07

    Optional: False

- **`insightDuration`**— la durata, espressa in minuti, di un evento Insights (il periodo di tempo dall'inizio alla fine dell'attività insolita sull'API oggetto). `insightDuration`si verifica sia negli eventi Insights di inizio che di fine.

  Since: 1.07

  Optional: False

- **`baselineDuration`**— la durata, espressa in minuti, del periodo di riferimento (il periodo di tempo in cui l'attività normale è misurata sull'API oggetto). `baselineDuration`è almeno i sette giorni (10080 minuti) che precedono un evento Insights. Questo campo è presente sia negli eventi Insights di inizio che di fine. L'ora di fine di `baselineDuration` è sempre l'inizio di un evento Insights.

  Since: 1.07

  Optional: False

- **`attributions`**: include informazioni sulle identità utente, sugli agenti dell'utente e sui codici di errore correlati all'attività insolita e di riferimento. Sono acquisiti un massimo di cinque identità utente, cinque agenti dell'utente e cinque codici di errore in un blocco `attributions` di un evento Insights, ordinati in base alla media del conteggio delle attività, in ordine decrescente dalla più alta alla più bassa.

  Since: 1.07

  Optional: True

  - **`attribute`**— Contiene il tipo di attributo. Il valore può essere `userIdentityArn`, `userAgent` o `errorCode`. Se presenti, questi valori verranno visualizzati una sola volta in un singolo attributo. Valori di attributo diversi possono avere `errorCode` valori `userIdentityArnuserAgent`, o diversi, ma ogni istanza di attributo conterrà solo un valore per `userIdentityArnuserAgent`, `oerrorCode`.

    Since: 1.07

    Optional: False

  - **`insight`**: un blocco che mostra fino ai primi cinque valori degli attributi che hanno contribuito alle chiamate o agli errori API commessi durante il periodo di attività insolita, in ordine decrescente dal numero di chiamate o errori API maggiore a quello minore. Mostra anche il numero medio di chiamate o errori API effettuati dai valori degli attributi durante il periodo di attività insolita.

    Since: 1.07

    Optional: False

    - **`value`**: l'attributo che ha contribuito alle chiamate o agli errori API commessi durante il periodo di attività insolita.

      Since: 1.07

      Facoltativo: falso falso

    - **`average`**: il numero di chiamate o errori API al minuto durante il periodo di attività insolita per l'attributo nel `value` campo.

      Since: 1.07

      Facoltativo: falso falso

- **`baseline`**: un blocco che mostra fino ai primi cinque valori degli attributi che hanno contribuito maggiormente alle chiamate o agli errori API durante il periodo di attività normale, in ordine decrescente dal numero di chiamate o errori API maggiore a quello minore. Mostra anche il numero medio di chiamate o errori API effettuati dai valori degli attributi durante il periodo di attività normale.

  Since: 1.07

  Facoltativo: falso falso

  - **`value`**: l'attributo che ha contribuito alle chiamate o agli errori API durante il periodo di attività normale.

    Since: 1.07

    Facoltativo: False False

  - **`average`**: la media cronologica delle chiamate o degli errori API al minuto durante i sette giorni precedenti all'ora di inizio dell'attività Insights per l'attributo nel `value` campo.

    Since: 1.07

    Facoltativo: False False

- **`eventCategory`**— La categoria dell'evento. Il valore è sempre relativo `Insight` agli eventi Insights.

  Since: 1.07

  Optional: False

Blocco **`insightDetails`** di esempio

Nell'esempio seguente viene illustrato un blocco `insightDetails` di evento Insights per un evento Insights che si è verificato quando l'API Application Auto Scaling `CompleteLifecycleAction` è stata chiamata un numero insolito di volte. Per un esempio di un evento Insights completo, consulta Eventi Insights.

Questo esempio proviene da un evento Insights di inizio, indicato da `"state": "Start"`. Le prime identità utente che hanno chiamato l'utente APIs associato all'evento Insights`CodeDeployRole1`,`CodeDeployRole2`, e`CodeDeployRole3`, sono mostrate nel `attributions` blocco, insieme alla frequenza media delle chiamate API per questo evento Insights

e al riferimento per il `CodeDeployRole1` ruolo. Il `attributions` blocco mostra anche che l'agente dell'utente è`codedeploy.amazonaws.com`, indicando che le prime identità utente hanno utilizzato la AWS CodeDeploy console per effettuare le chiamate API.

Poiché non sono presenti codici di errore associati agli eventi analizzati per generare l'evento Insights (il valore è `null`), la media `insight` per il codice di errore è la stessa della media `insight` generale per l'intero evento Insights, mostrata nel blocco `statistics`.

```
          "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
```

```
                    ],
                    "baseline": [
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "userAgent",
                    "insight": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "errorCode",
                    "insight": [
                      {
                        "value": "null",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "null",
                        "average": 0.0000882145
                      }
                    ]
                  }
                ]
              }
            }
```

CloudTrail registra i contenuti per gli eventi Insights per i datastore di eventi Lake.

AWS CloudTrail I record degli eventi Insights per i datastore di eventi includono campi diversi da altri CloudTrail eventi nella loro struttura JSON, a volte chiamati payload. Un record di eventi CloudTrail Insights per un data store di eventi include i seguenti campi:

> **Note**
>
> I `baselineAverage` campi `insightValueinsightAverage`,`baselineValue`, e all'interno del `attributions` campo di `insightContext` inizieranno a essere obsoleti il 23 giugno 2025.

- **`eventVersion`**— La versione del formato di registro degli eventi.

  Optional: False
- **`eventCategory`**— La categoria dell'evento. Il valore è sempre relativo `Insight` agli eventi Insights.

  Optional: False
- **`eventType`**— Il tipo di evento. Il valore è sempre `AwsCloudTrailInsight` per gli eventi Insights.

  Optional: False
- **`eventID`**: GUID generato da CloudTrail per identificare in modo univoco ogni evento. Puoi utilizzare questo valore per identificare un singolo evento. Ad esempio, puoi utilizzare l'ID come chiave primaria per recuperare i dati di log da un database ricercabile.

  Optional: False
- **`eventTime`**: l'ora in cui l'evento Insights ha avuto inizio o si è interrotto, espressa nel Tempo coordinato universale (UTC).

  Optional: False
- **`awsRegion`**— Il Regione AWS luogo in cui si è verificato l'evento Insights, ad esempio`us-east-2`.

  Optional: False

- **`recipientAccountId`**: rappresenta l'ID dell'account che ha ricevuto questo evento.

  Optional: True

- **`sharedEventID`**— Un GUID generato da CloudTrail Insights per identificare in modo univoco un evento Insights. `sharedEventID`è comune tra gli eventi Insights di inizio e di fine e consente di connettere entrambi gli eventi per identificare in modo univoco l'attività insolita. Puoi considerare lo `sharedEventID` come l'ID evento generale di Insights.

  Optional: False

- **`addendum`**: se la consegna di un evento ha subito un ritardo o se diventano disponibili ulteriori informazioni su un evento esistente dopo la registrazione dell'evento, un campo addendum mostra informazioni sul motivo per cui l'evento ha subito un ritardo. Se mancavano informazioni da un evento esistente, il campo addendum include le informazioni mancanti e un motivo per cui mancavano. Consulta anche `addendum` in CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

  Optional: True

- **`insightSource`**— L'archivio dati degli eventi di origine che ha raccolto gli eventi di gestione analizzati.

  Optional: False

- **`insightState`**: indica se l'evento è l'evento Insights di inizio o di fine. Il valore può essere `Start` o `End`.

  Optional: False

- **`insightEventSource`**— Servizio AWS Quella era la fonte dell'attività insolita, ad esempio`ec2.amazonaws.com`.

  Optional: False

- **`insightEventName`**: il nome dell'evento Insights, in genere il nome dell'API che ha dato origine all'attività insolita.

  Optional: False

- **`insightErrorCode`**— Il codice di errore dell'attività insolita. Consulta anche `errorCode` in CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

  Optional: True

- **`insightType`**— Il tipo di evento Insights. Questo valore può essere `ApiCallRateInsight` o `ApiErrorRateInsight`.

  Optional: False

- **`insightContext`**— Contiene informazioni sul fattore scatenante alla base di un evento Insights, come l'identità dell'utente, lo user agent, la media o la baseline storica e la durata e la media di Insights.

  Optional: False

  - **`baselineAverage`**: il numero medio di chiamate o errori API al minuto per la durata di riferimento all'API oggetto dell'evento Insights per l'account, calcolato nei sette giorni precedenti all'inizio dell'evento Insights.

    Optional: False

  - **`insightAverage`**: per un evento Insights di inizio, questo valore è il numero medio di chiamate o errori API al minuto durante l'inizio dell'attività insolita. Per un evento Insights di fine, questo valore è il numero medio di chiamate o erriri API al minuto per la durata dell'attività insolita.

    Optional: False

  - **`baselineDuration`**— La durata, espressa in minuti, del periodo di riferimento (il periodo di tempo in cui l'attività normale è misurata sull'API oggetto). `baselineDuration`è almeno i sette giorni (10080 minuti) che precedono un evento Insights. Questo campo è presente sia negli eventi Insights di inizio che di fine. L'ora di fine di `baselineDuration` è sempre l'inizio di un evento Insights.

    Optional: False

  - **`insightDuration`**— La durata, espressa in minuti, di un evento Insights (il periodo di tempo dall'inizio alla fine dell'attività insolita sull'API oggetto). `insightDuration`si verifica sia negli eventi Insights di inizio che di fine.

    Optional: False

  - **`attributions`**: include informazioni sull'identità utente, sull'agente dell'utente o sul codice di errore correlati all'attività insolita e di riferimento.

    Optional: True

> **Note**
>
> I `baselineAverage` campi `insightValueinsightAverage`,`baselineValue`, e all'interno del `attributions` campo di `insightContext` inizieranno a essere obsoleti il 23 giugno 2025.

- **`attribute`**— Contiene il tipo di attributo. Il valore può essere `userIdentityArn`, `userAgent` o `errorCode`. Se presenti, questi valori verranno visualizzati una sola volta in un singolo attributo. Valori di attributo diversi possono avere `errorCode` valori `userIdentityArnuserAgent`, o diversi, ma ogni istanza di attributo conterrà solo un valore per `userIdentityArnuserAgent`, `oerrorCode`.

  Optional: False
- **`insightValue`**: il valore dell'attributo principale che si è verificato nelle chiamate o negli errori API effettuati durante il periodo di attività insolita.

  Optional: False
- **`insightAverage`**: il numero di chiamate o errori API al minuto durante il periodo di attività insolita per l'attributo nel `insightValue` campo.

  Optional: False
- **`baselineValue`**: il valore dell'attributo principale che ha contribuito alle chiamate o agli errori API registrati durante il periodo di attività normale.

  Optional: False
- **`baselineAverage`**: la media cronologica delle chiamate o degli errori API al minuto durante i sette giorni precedenti all'ora di inizio dell'attività Insights per l'attributo nel `baselineValue` campo.

  Optional: False
- **`insight`**: i primi cinque valori degli attributi che hanno contribuito alle chiamate o agli errori API commessi durante il periodo di attività insolita. Mostra anche il numero medio di chiamate o errori API effettuati dall'attributo durante il periodo di attività insolita.

  Optional: False

- **`value`**: l'attributo che ha contribuito alle chiamate o agli errori API effettuati durante il periodo di attività insolita.

  Optional: False

- **`average`**: il numero medio di chiamate o errori API al minuto durante il periodo di attività insolita per l'attributo nel `value` campo.

  Optional: False

- **`baseline`**: i primi cinque valori degli attributi che hanno contribuito maggiormente alle chiamate o agli errori API durante il periodo di attività normale. Mostra anche il numero medio di chiamate o errori API registrati dal valore dell'attributo durante il periodo di attività normale.

  Optional: False

  - **`value`**: l'attributo che ha contribuito alle chiamate o agli errori API durante il periodo di attività normale.

    Optional: False

  - **`average`**: la media cronologica delle chiamate o degli errori API al minuto durante i sette giorni precedenti all'ora di inizio dell'attività Insights per l'attributo nel `value` campo.

    Optional: False

CloudTrail elemento userIdentity

AWS Identity and Access Management (IAM) fornisce diversi tipi di identità. L'elemento `userIdentity` include dettagli sul tipo di identità IAM che ha effettuato la richiesta e sulle credenziali utilizzate. Se sono state utilizzate credenziali temporanee, l'elemento mostra il modo in cui tali credenziali sono state ottenute.

Indice

- Esempi
- Campi
- Valori per AWS STS APIs con SAML e la federazione delle identità web
- AWS STS identità di origine

Esempi

`userIdentity` con credenziali utente IAM

L'esempio seguente mostra l'elemento `userIdentity` di una semplice richiesta effettuata con le credenziali dell'utente IAM denominato `Alice`.

```
"userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJ45Q7YFFAREXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Alice"
}
```

`userIdentity` con credenziali di sicurezza temporanee

L'esempio seguente mostra un elemento `userIdentity` per una richiesta effettuata con le credenziali di sicurezza temporanee ottenute mediante l'assunzione del ruolo IAM. L'elemento contiene ulteriori dettagli sul ruolo assunto per ottenere le credenziali.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAIDPPEZS35WEXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
            "accountId": "123456789012",
            "userName": "RoleToBeAssumed"
        },
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    }
}
```

`userIdentity` per una richiesta effettuata per conto di un utente del Centro identità IAM

L'esempio seguente mostra un elemento `userIdentity` per una richiesta effettuata per conto di un utente del Centro identità IAM.

```
"userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "123456789012",
    "onBehalfOf": {
        "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9067642ac7"
    },
    "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

Per ulteriori informazioni su come utilizzare e `userId` `identityStoreArn``credentialId`, consulta Identificazione dell'utente e della sessione negli eventi avviati dall' CloudTrail utente di IAM Identity Center nella Guida per l'utente di IAM Identity Center.

Campi

In un elemento `userIdentity` possono essere visualizzati i seguenti campi.

`type`

Tipo dell'identità. I valori possibili sono i seguenti:

- `Root`— La richiesta è stata effettuata con Account AWS le tue credenziali. Se il tipo di `userIdentity` è `Root` e imposti un alias per il tuo account, il campo `userName` conterrà l'alias del tuo account. Per ulteriori informazioni, consulta ID account Account AWS e relativo alias.
- `IAMUser` – La richiesta è stata effettuata con le credenziali di un utente IAM.
- `AssumedRole` – La richiesta è stata effettuata con le credenziali di sicurezza temporanee ottenute con un ruolo tramite una chiamata all'API AWS Security Token Service (AWS STS)`AssumeRole`. Ciò può includere ruoli per Amazon EC2 e accesso alle API tra account.
- `Role` – La richiesta è stata effettuata con un'identità IAM persistente che dispone delle autorizzazioni specifiche. L'emittente delle sessioni di ruolo è sempre il ruolo. Per ulteriori informazioni sui ruoli consulta Termini e concetti dei ruoli nella Guida per l'utente IAM.

- `FederatedUser`— La richiesta è stata effettuata con credenziali di sicurezza temporanee ottenute da una chiamata all' AWS STS `GetFederationToken`API. L'elemento `sessionIssuer` indica se l'API è stata chiamata con le credenziali dell'utente root o con quelle dell'utente IAM.

  Per ulteriori informazioni sulle credenziali di sicurezza temporanee, consulta la sezione relativa alle credenziali di sicurezza temporanee nella Guida per l'utente IAM.
- `Directory` - La richiesta è stata effettuata a un servizio directory e il tipo è sconosciuto. I servizi di directory includono: Amazon WorkDocs e Amazon QuickSight.
- `AWSAccount`— La richiesta è stata fatta da un altro Account AWS
- `AWSService`— La richiesta è stata fatta da un Account AWS uomo che appartiene a un Servizio AWS. Ad esempio, AWS Elastic Beanstalk presuppone un ruolo IAM nel tuo account per chiamare altre persone per tuo Servizi AWS conto.
- `IdentityCenterUser`: la richiesta è stata effettuata per conto di un utente del Centro identità IAM
- `Unknown`— La richiesta è stata effettuata con un tipo di identità che non è CloudTrail possibile determinare.

Optional: False

Vengono visualizzati i valori `AWSAccount` e `AWSService` nel campo `type` dei log in caso di accesso tra più account tramite un ruolo IAM di tua proprietà.

Esempio: accesso multiaccount avviato da un altro account AWS

1. Tu sei il proprietario di un ruolo IAM nel tuo account.
2. Un altro AWS account passa a quel ruolo per assumere il ruolo del tuo account.
3. Poiché sei il proprietario del ruolo IAM, riceverai un log che mostra l'altro account che ha assunto il ruolo. Il valore del campo `type` è `AWSAccount`. Per un esempio di immissione di registro, consulta AWS STS l'evento API nel file di CloudTrail registro.

Esempio: accesso tra account diversi avviato da un servizio AWS

1. Tu sei il proprietario di un ruolo IAM nel tuo account.
2. Un AWS account di proprietà di un AWS servizio assume tale ruolo.
3. Poiché sei il proprietario del ruolo IAM, riceverai un log che mostra il servizio AWS che ha assunto il ruolo. Il valore del campo `type` è `AWSService`.

`userName`

Nome descrittivo dell'identità che ha effettuato la chiamata. Il valore visualizzato nel campo `userName` si basa sul valore di `type`. La tabella seguente mostra la relazione tra `type` e `userName`:

`type`	**`userName`**	Descrizione
`Root` (nessun alias impostato)	Non presente	Se non hai impostato un alias per il tuo Account AWS, il `userName` campo non viene visualizzato. Per ulteriori informazioni sugli alias degli account, vedi Il tuo Account AWS ID e il suo alias. Il campo `userName` non può contenere `Root` perché `Root` è un tipo di identità e non un nome utente.
`Root` (alias impostato)	Alias dell'account	Per ulteriori informazioni sugli Account AWS alias, vedi Il tuo Account AWS ID e il suo alias.
`IAMUser`	Nome utente dell'utente IAM	
`AssumedRole`	Non presente	Per il `AssumedRole` tipo, è possibile trovare il `userName` campo in `sessionContext` come parte dell'elemento sessionIssuer. Per una voce di esempio, consulta Esempi.
`Role`	Definito dall'utente	Le sezioni `sessionContext` e `sessionIssuer` contengono informazioni sull'identità che ha creato la sessione per il ruolo.
`FederatedUser`	Non presente	Le sezioni `sessionContext` e `sessionIssuer` contengono informazioni sull'identità che ha creato la sessione per l'utente federato.
`Directory`	Può essere presente	Ad esempio, il valore può essere l'alias dell'account o l'indirizzo e-mail dell'ID account Account AWS associato.
`AWSService`	Non presente	

type	userName	Descrizione
AWSAccount	Non presente	
IdentityCenterUser	Non presente*	La sezione onBehalfOf contiene informazioni sull'ID utente del Centro identità IAM e sull'ARN dell'archivio di identità per cui è stata effettuata la chiamata. Per ulteriori informazioni su come utilizzare questi due campi, consulta Identificazione dell'utente e della sessione negli eventi avviati dall' CloudTrail utente di IAM Identity Center nella Guida per l'utente di IAM Identity Center. * IAM Identity Center emette il userName campo sotto l'additionalEventData elemento in due eventi di accesso CloudTrail . Per ulteriori informazioni, consulta Username negli CloudTrail eventi di accesso nella Guida per l'utente di IAM Identity Center.
Unknown	Può essere presente	Ad esempio, il valore può essere l'alias dell'account o l'indirizzo e-mail dell'ID account Account AWS associato.

> **Note**
>
> Il campo userName contiene la stringa HIDDEN_DUE_TO_SECURITY_REASONS quando l'evento registrato corrisponde a un errore di accesso alla console causato dall'immissione errata del nome utente. In questo caso CloudTrail non registra i contenuti perché il testo potrebbe contenere informazioni sensibili, come negli esempi seguenti:
>
> - Un utente ha immesso accidentalmente una password nel campo del nome utente.
> - Un utente fa clic sul collegamento della pagina di accesso di un AWS account, ma poi digita il numero di account per un altro account.

- Un utente immette accidentalmente il nome account di un account e-mail personale, un identificatore di accesso alla banca o a un altro ID privato.

Optional: True

principalId

Identificatore univoco per l'entità che ha effettuato la chiamata. Per le richieste effettuate con le credenziali di sicurezza temporanee, questo valore include il nome di sessione passato alla chiamata API `AssumeRole`, `AssumeRoleWithWebIdentity`o `GetFederationToken`.

Optional: True

arn

ARN (Amazon Resource Name) dell'entità che ha effettuato la chiamata. L'ultima sezione dell'ARN contiene l'utente o il ruolo che ha effettuato la chiamata.

Optional: True

accountId

Account che possiede l'entità che ha concesso le autorizzazioni per la richiesta. Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, corrisponde all'account proprietario dell'utente o del ruolo IAM utilizzato per ottenere le credenziali.

Se la richiesta è stata effettuata con un token di accesso autorizzato del Centro identità IAM, questo è l'account proprietario dell'istanza del Centro identità IAM.

Optional: True

accessKeyId

ID della chiave di accesso utilizzata per firmare la richiesta. Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, corrisponde all'ID della chiave di accesso delle credenziali temporanee. Per motivi di sicurezza, `accessKeyId` potrebbe non essere presente o potrebbe essere visualizzato come una stringa vuota.

Optional: True

sessionContext

Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee, `sessionContext` fornisce informazioni sulla sessione creata per tali credenziali. Le sessioni vengono create

quando viene chiamata una qualsiasi API che restituisce le credenziali temporanee. Gli utenti creano anche sessioni quando lavorano nella console ed effettuano richieste APIs che includono l'autenticazione a più fattori. I seguenti attributi possono essere visualizzati in `sessionContext`:

- `sessionIssuer`— Se un utente effettua una richiesta con credenziali di sicurezza temporanee, `sessionIssuer` fornisce informazioni su come l'utente ha ottenuto le credenziali. Ad esempio, se le credenziali di sicurezza temporanee sono state ottenute mediante l'assunzione di un ruolo, questo elemento fornisce informazioni sul ruolo assunto. Se le credenziali sono state ottenute con credenziali root o dell'utente IAM per effettuare la chiamata a AWS STS `GetFederationToken`, l'elemento fornisce informazioni sull'account root o sull'utente IAM. Questo elemento ha i seguenti attributi:
  - `type` - L'origine delle credenziali di sicurezza temporanee, ad esempio `Root`,`IAMUser` o `Role`.
  - `userName` - Il nome descrittivo dell'utente o del ruolo che ha creato la sessione. Il valore visualizzato dipende dal valore dell'identità `sessionIssuer type`. La tabella seguente mostra la relazione tra `sessionIssuer type` e `userName`:

`sessionIssuer` tipo	**`userName`**	Descrizione
`Root` (nessun alias impostato)	Non presente	Se non hai configurato un alias per il tuo account, il campo `userName` non viene visualizzato. Per ulteriori informazioni sugli Acc ount AWS alias, consulta Your Account AWS ID e relativo alias. Il campo `userName` non può contenere `Root` perché `Root` è un tipo di identità e non un nome utente.
`Root` (alias impostato)	Alias dell'account	Per ulteriori informazioni sugli Account AWS alias, vedi L'ID AWS dell'account e il relativo alias.
`IAMUser`	Nome utente dell'utente IAM	Valido anche quando un utente federato utilizza una sessione creata da `IAMUser`.

sessionIssuer tipo	**userName**	Descrizione
`Role`	Nome del ruolo	Un ruolo assunto da un utente IAM o da un utente federato con identità web in una sessione di ruolo. Servizio AWS

  - `principalId`: l'ID interno dell'entità utilizzata per ottenere le credenziali.
  - `arn` - L'ARN dell'origine (account, utente IAM o ruolo) utilizzata per ottenere le credenziali di sicurezza temporanee.
  - `accountId` - L'account proprietario dell'entità utilizzata per ottenere le credenziali.
- `webIdFederationData`— Se la richiesta è stata effettuata con credenziali di sicurezza temporanee ottenute dalla federazione delle identità web, `webIdFederationData` elenca le informazioni sul provider di identità.

  Questo elemento ha i seguenti attributi:

  - `federatedProvider` - Il nome entità del provider di identità (ad esempio, `www.amazon.com` per Login with Amazon o `accounts.google.com` per Google).
  - `attributes` - L'ID applicazione e l'ID utente forniti dal provider (ad esempio, `www.amazon.com:app_id` e `www.amazon.com:user_id` per Login with Amazon).

  > **Note**
  >
  > L'omissione di questo campo o la presenza di questo campo con un valore vuoto indica che non ci sono informazioni sul provider di identità.

- `assumedRoot`— Il valore si riferisce `true` a una sessione temporanea quando un account di gestione o un amministratore delegato chiama. AWS STS `AssumedRoot` Per ulteriori informazioni, consulta Track Privileged Tasks CloudTrail nella IAM User Guide. Questo campo è opzionale.
- `attributes`— Gli attributi della sessione.
  - `creationDate` - La data e l'ora in cui le credenziali di sicurezza temporanee sono state generate. Valore rappresentato nella notazione di base ISO 8601.
  - `mfaAuthenticated`: il valore è `true` se anche l'utente root o l'utente IAM le cui credenziali sono state utilizzate per la richiesta è stato autenticato con un dispositivo MFA. In caso contrario, il valore è `false`.

- `sourceIdentity` - Consulta AWS STS identità di origine in questo argomento. Il campo `sourceIdentity` è presente negli eventi in cui gli utenti assumono un ruolo IAM per eseguire un'azione. `sourceIdentity` identifica l'identità dell'utente originale che effettua la richiesta, indipendentemente dal fatto che l'identità dell'utente sia un utente IAM, un ruolo IAM, un utente autenticato utilizzando la federazione basata su SAML o un utente autenticato utilizzando la federazione delle identità Web compatibile con OpenID Connect (OIDC). Per ulteriori informazioni sulla configurazione AWS STS per la raccolta delle informazioni sull'identità di origine, consulta Monitoraggio e controllo delle azioni intraprese con i ruoli assunti nella Guida per l'utente IAM.
- `ec2RoleDelivery`— Il valore è `1.0` se le credenziali sono state fornite da Amazon EC2 Instance Metadata Service versione 1 ()IMDSv1. Il valore è `2.0` se le credenziali sono state fornite utilizzando il nuovo schema di IMDS.

  AWS le credenziali fornite da Amazon EC2 Instance Metadata Service (IMDS) includono una chiave di contesto ec2: RoleDelivery IAM. Questa chiave di contesto semplifica l'applicazione del nuovo schema su resource-by-resource base service-by-service OR utilizzando la chiave di contesto come condizione nelle politiche IAM, nelle politiche delle risorse o nelle politiche di controllo dei servizi. AWS Organizations Per ulteriori informazioni, consulta Metadati dell'istanza e dati utente nella Amazon EC2 User Guide.

Optional: True

`invokedBy`

Il nome di chi Servizio AWS ha effettuato la richiesta, quando una richiesta viene effettuata da un soggetto Servizio AWS come Amazon EC2 Auto Scaling o. AWS Elastic Beanstalk Questo campo è presente solo quando una richiesta viene effettuata da un Servizio AWS. Ciò include le richieste effettuate dai servizi che utilizzano sessioni di accesso inoltrato (FAS), Servizio AWS principali, ruoli collegati ai servizi o ruoli di servizio utilizzati da un. Servizio AWS

Optional: True

`onBehalfOf`

Se la richiesta è stata effettuata da un chiamante del Centro identità IAM, `onBehalfOf` fornisce informazioni sull'ID utente del Centro identità IAM e sull'ARN dell'archivio di identità per cui è stata effettuata la chiamata. Questo elemento ha i seguenti attributi:

- `userId`: l'ID dell'utente del Centro identità IAM per cui è stata effettuata la chiamata.
- `identityStoreArn`: l'ARN dell'archivio di identità del Centro identità IAM per cui è stata effettuata la chiamata.

Optional: True

inScopeOf

Se la richiesta è stata effettuata nell'ambito di un Servizio AWS, ad esempio Lambda o Amazon ECS, fornisce informazioni sulla risorsa o sulle credenziali relative alla richiesta. Questo elemento può contenere i seguenti attributi:

- `sourceArn`— L'ARN della risorsa che ha richiamato la richiesta. service-to-service
- `sourceAccount`— L'ID dell'account proprietario per. `sourceArn` Viene visualizzato insieme a`sourceArn`.
- `issuerType`— Il tipo di risorsa di`credentialsIssuedTo`. Ad esempio, `AWS::Lambda::Function`.
- `credentialsIssuedTo`— La risorsa relativa all'ambiente in cui sono state emesse le credenziali.

Optional: True

credentialId

L'ID delle credenziali per la richiesta. Viene impostato solo quando il chiamante utilizza un token portante, ad esempio un token di accesso autorizzato dal Centro identità IAM.

Optional: True

Valori per AWS STS APIs con SAML e la federazione delle identità web

AWS CloudTrail supporta le chiamate API logging AWS Security Token Service (AWS STS) effettuate con Security Assertion Markup Language (SAML) e la federazione delle identità web. Quando un utente effettua una chiamata verso la rete `AssumeRoleWithSAML``AssumeRoleWithWebIdentity` APIs, CloudTrail registra la chiamata e invia l'evento al tuo bucket Amazon S3.

L'`userIdentity`elemento corrispondente APIs contiene i seguenti valori.

type

Tipo di identità.

- `SAMLUser` - La richiesta è stata effettuata con un'asserzione SAML.

- `WebIdentityUser` - La richiesta è stata effettuata da un provider di federazioni di identità Web.

`principalId`

Identificatore univoco per l'entità che ha effettuato la chiamata.

- Per `SAMLUser`, corrisponde a una combinazione delle chiavi `saml:namequalifier` e `saml:sub`.
- Per `WebIdentityUser`, corrisponde a una combinazione di approvatore, ID applicazione e ID utente.

`userName`

Nome dell'identità che ha effettuato la chiamata.

- Per `SAMLUser`, corrisponde alla chiave `saml:sub`.
- Per `WebIdentityUser`, corrisponde all'ID utente.

`identityProvider`

Nome entità del provider di identità esterne. Questo campo viene visualizzato solo per i tipi `SAMLUser` o `WebIdentityUser`.

- Per `SAMLUser`, corrisponde alla chiave `saml:namequalifier` per l'asserzione SAML.
- Per `WebIdentityUser`, corrisponde al nome approvatore del provider di federazioni di identità Web. Può essere un provider che hai configurato, ad esempio:
  - `cognito-identity.amazon.com` per Amazon Cognito
  - `www.amazon.com` per Login with Amazon
  - `accounts.google.com` per Google
  - `graph.facebook.com` per Facebook

Di seguito è illustrato un elemento `userIdentity` di esempio per l'operazione `AssumeRoleWithWebIdentity`.

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-
id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
```

```
}
```

Ad esempio, i log di come l'`userIdentity`elemento appare `SAMLUser` e i `WebIdentityUser` tipi, vedi Registrazione delle chiamate IAM e AWS STS API con. AWS CloudTrail

AWS STS identità di origine

Un amministratore IAM può configurare la configurazione AWS Security Token Service in modo da richiedere agli utenti di specificare la propria identità quando utilizzano credenziali temporanee per assumere ruoli. Il campo `sourceIdentity` è presente negli eventi in cui gli utenti assumono un ruolo IAM o eseguono azioni con il ruolo assunto.

Il campo `sourceIdentity` identifica l'identità dell'utente originale che effettua la richiesta, indipendentemente dal fatto che l'identità dell'utente sia un utente IAM, un ruolo IAM, un utente autenticato utilizzando la federazione basata su SAML o un utente autenticato utilizzando la federazione delle identità Web compatibile con OpenID Connect (OIDC). Dopo la configurazione AWS STS, l'amministratore IAM CloudTrail registra `sourceIdentity` le informazioni nei seguenti eventi e luoghi all'interno del record dell'evento:

- Le `AssumeRoleWithWebIdentity` chiamate AWS STS `AssumeRoleAssumeRoleWithSAML`, o eseguite da un'identità utente quando assume un ruolo. `sourceIdentity`si trova nel `requestParameters` blocco delle AWS STS chiamate.
- Le `AssumeRoleWithWebIdentity` chiamate AWS STS `AssumeRoleAssumeRoleWithSAML`, or eseguite da un'identità utente se utilizza un ruolo per assumere un altro ruolo, noto come concatenamento dei ruoli. `sourceIdentity`si trova nel `requestParameters` blocco delle AWS STS chiamate.
- L'API AWS di servizio effettua le chiamate effettuate dall'identità dell'utente assumendo un ruolo e utilizzando le credenziali temporanee assegnate da. AWS STS Negli eventi API di servizio, `sourceIdentity` è presente nel blocco `sessionContext`. Ad esempio, se un'identità utente crea un nuovo bucket S3, `sourceIdentity` si verifica nel blocco `sessionContext` dell'evento `CreateBucket`.

Per ulteriori informazioni su come configurare la raccolta di informazioni sull'identità AWS STS di origine, consulta Monitorare e controllare le azioni intraprese con i ruoli assunti nella Guida per l'utente IAM. Per ulteriori informazioni sugli AWS STS eventi registrati CloudTrail, consulta Logging IAM and AWS STS API call with AWS CloudTrail the IAM User Guide.

Di seguito sono riportati frammenti di esempio di eventi che mostrano il campo `sourceIdentity`.

Sezione di esempio **`requestParameters`**

Nel seguente esempio di frammento di evento, un utente effettua una AWS STS `AssumeRole` richiesta e imposta un'identità di origine, qui rappresentata da. *`source-identity-value-set`* L'utente assume un ruolo rappresentato dal ruolo ARN `arn:aws:iam::123456789012:role/Assumed_Role`. Il campo `sourceIdentity` è presente nel blocco `requestParameters` dell'evento.

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

Sezione di esempio **`responseElements`**

Nel frammento di evento di esempio seguente, un utente AWS STS `AssumeRole` richiede di assumere un ruolo denominato e imposta un'identità di origine`Developer_Role`,. `Admin` L'utente assume un ruolo rappresentato dal ruolo ARN `arn:aws:iam::111122223333:role/Developer_Role`. Il campo `sourceIdentity` è presente nel blocco `requestParameters` e `responseElements` dell'evento. Le credenziali temporanee utilizzate per assumere il ruolo, la stringa del token di sessione e l'ID del ruolo assunto, il nome della sessione e l'ARN della sessione sono mostrati nel blocco `responseElements`, insieme all'identità di origine.

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
```

```
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                             EXAMPLE_SESSION_TOKEN
                             XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

Sezione di esempio **`sessionContext`**

Nel frammento di evento di esempio seguente, un utente assume un ruolo denominato `DevRole` per chiamare un'API di servizio. AWS L'utente imposta un'identità di origine, qui rappresentata da. *`source-identity-value-set`* Il campo `sourceIdentity` è presente nel blocco `sessionContext` dell'evento `userIdentity`.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
```

```
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

Eventi non API acquisiti da CloudTrail

Oltre a registrare le chiamate AWS API, CloudTrail registra altri eventi correlati che potrebbero avere un impatto sulla sicurezza o sulla conformità sull' AWS account o che potrebbero aiutarti a risolvere problemi operativi.

- Servizio AWS eventi: CloudTrail supporta la registrazione di eventi di servizio non API. Questi eventi vengono creati dai AWS servizi ma non vengono attivati direttamente da una richiesta a un'API pubblica. AWS Per questi eventi, il campo `eventType` è `AwsServiceEvent`.
- AWS Management Console eventi di accesso: CloudTrail registra i tentativi di accesso ai AWS Management Console, ai Forum di AWS discussione e al AWS Support Center. Tutti gli eventi di accesso degli utenti e degli utenti root di IAM, nonché tutti gli eventi di accesso degli utenti federati, generano record. CloudTrail Per gli eventi di accesso, il campo è. `eventType` `AwsConsoleSignIn`

Servizio AWS eventi

CloudTrail supporta la registrazione di eventi di servizio non API. Questi eventi vengono creati dai AWS servizi ma non vengono attivati direttamente da una richiesta a un'API pubblica. AWS Per questi eventi, il campo `eventType` è `AwsServiceEvent`.

Di seguito è riportato uno scenario di esempio di un evento di AWS servizio in cui una chiave gestita dal cliente viene ruotata automaticamente in AWS Key Management Service ()AWS KMS. Per ulteriori informazioni sulla rotazione delle chiavi KMS, consulta Rotazione delle chiavi KMS.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

AWS Management Console eventi di accesso

CloudTrail registra i tentativi di accesso ai AWS Management Console, ai Forum di AWS discussione e al AWS Support Center. Tutti gli eventi di accesso degli utenti e degli utenti root IAM, nonché tutti gli eventi di accesso degli utenti federati, generano record nei file di registro. CloudTrail Per informazioni sulla ricerca e la visualizzazione dei file di log, consulta Trovare i file di registro CloudTrail e Scaricamento dei file di CloudTrail registro.

Puoi utilizzarlo Notifiche all'utente AWSper configurare i canali di distribuzione per ricevere notifiche sugli eventi. AWS CloudTrail L'utente riceverà una notifica quando un evento corrisponde a una regola specificata. Puoi ricevere notifiche relative agli eventi attraverso più canali, tra cui e-mail, Amazon Q Developer in chat, applicazioni di chat, notifiche di chat o notifiche AWS Console Mobile Applicationpush. Puoi anche visualizzare le notifiche nel Centro notifiche della console. Notifiche all'utente supporta l'aggregazione, che può ridurre il numero di notifiche ricevute durante eventi specifici.

> **Note**
>
> La regione registrata in un `ConsoleLogin` evento varia in base al tipo di utente e al fatto che utilizzi un endpoint globale o regionale per accedere.
>
> - Se accedi come utente root, CloudTrail registra l'evento in us-east-1.
> - Se accedi con un utente IAM e utilizzi l'endpoint globale, CloudTrail registra la regione dell'`ConsoleLogin`evento come segue:
> - Se nel browser è presente un cookie di alias dell'account, CloudTrail registra l'`ConsoleLogin`evento in una delle seguenti regioni: us-east-2, eu-north-1 o ap-southeast-2. Questo perché il proxy della console reindirizza l'utente in base alla latenza dalla posizione di accesso dell'utente.
> - Se nel browser non è presente un cookie di alias dell'account, CloudTrail registra l'`ConsoleLogin`evento in us-east-1. Questo perché il proxy della console reindirizza nuovamente all'accesso globale.
> - Se accedi con un utente IAM e utilizzi un endpoint regionale, CloudTrail registra l'`ConsoleLogin`evento nella regione appropriata per l'endpoint. Per ulteriori informazioni sugli Accedi ad AWS endpoint, consulta Accedi ad AWS endpoints and quote.

Argomenti

- Record di eventi di esempio per gli utenti IAM
- Record di evento di esempio per gli utenti root
- Record di eventi di esempio per gli utenti federati

Record di eventi di esempio per gli utenti IAM

Negli esempi seguenti vengono illustrati i record di eventi per diversi scenari di accesso dell'utente IAM.

Argomenti

- Utente IAM, accesso effettuato correttamente senza MFA
- Utente IAM, accesso effettuato correttamente con MFA
- Utente IAM, accesso non riuscito
- Utente IAM, controlli del processo di accesso per MFA (singolo tipo di dispositivo MFA)

- Utente IAM, controlli del processo di accesso per MFA (più tipi di dispositivi MFA)

Utente IAM, accesso effettuato correttamente senza MFA

Il record seguente mostra che un utente denominato ha effettuato `Anaya` correttamente l'accesso AWS Management Console senza utilizzare l'autenticazione a più fattori (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
```

```
    }
}
```

Utente IAM, accesso effettuato correttamente con MFA

Il record seguente mostra che un utente IAM denominato ha effettuato `Anaya` correttamente l'accesso all' AWS Management Console autenticazione a più fattori (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
```

```
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utente IAM, accesso non riuscito

Il record seguente mostra un tentativo di accesso non riuscito da parte dell'utente IAM denominato `Paulo`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
```

```
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utente IAM, controlli del processo di accesso per MFA (singolo tipo di dispositivo MFA)

Quanto segue mostra che il processo di accesso ha controllato se l'autenticazione a più fattori (MFA) è richiesta per un utente IAM durante l'accesso. In questo esempio, il valore di `mfaType` è `U2F MFA`, che indica che l'utente IAM ha abilitato un singolo dispositivo MFA o più dispositivi MFA dello stesso tipo (`U2F MFA`).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
```

```
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Utente IAM, controlli del processo di accesso per MFA (più tipi di dispositivi MFA)

Quanto segue mostra che il processo di accesso ha controllato se l'autenticazione a più fattori (MFA) è richiesta per un utente IAM durante l'accesso. In questo esempio, il valore di `mfaType` è `Multiple MFA Devices`, che indica che l'utente IAM ha abilitato più tipi di dispositivi MFA.

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "IAMUser",
       "principalId": "EXAMPLE6E4XEGITWATV6R",
       "accountId": "123456789012",
       "accessKeyId": "",
       "userName": "Mary"
   },
   "eventTime": "2023-07-19T23:10:09Z",
   "eventSource": "signin.amazonaws.com",
   "eventName": "CheckMfa",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "192.0.2.0",
   "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
   "requestParameters": null,
   "responseElements": {
       "CheckMfa": "Success"
   },
   "additionalEventData": {
       "MfaType": "Multiple MFA Devices"
   },
   "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
   "readOnly": false,
   "eventType": "AwsConsoleSignIn",
   "managementEvent": true,
   "recipientAccountId": "123456789012",
   "eventCategory": "Management",
   "tlsDetails": {
```

```
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Record di evento di esempio per gli utenti root

Negli esempi seguenti vengono illustrati i record di eventi per diversi scenari di accesso dell'utente `root`. Quando si accede utilizzando l'utente root, CloudTrail registra l'`ConsoleLogin`evento in us-east-1.

Argomenti

- Utente root, accesso effettuato correttamente senza MFA
- Utente root, accesso effettuato correttamente con MFA
- Utente root, accesso non riuscito
- Utente root, MFA modificata
- Utente root, password modificata

Utente root, accesso effettuato correttamente senza MFA

Di seguito viene illustrato un evento di accesso riuscito per un utente root che non utilizza l'autenticazione a più fattori (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Utente root, accesso effettuato correttamente con MFA

Di seguito viene illustrato un evento di accesso riuscito per un utente root con l'autenticazione a più fattori (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Utente root, accesso non riuscito

Di seguito viene illustrato un evento di accesso non riuscito per un utente root che non utilizza MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Utente root, MFA modificata

Di seguito viene illustrato un evento di esempio per un utente root che modifica le impostazioni dell'autenticazione a più fattori (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Utente root, password modificata

Di seguito viene illustrato un evento di esempio per un utente root che modifica la password.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

Record di eventi di esempio per gli utenti federati

Negli esempi seguenti vengono illustrati i record di eventi per gli utenti federati. Agli utenti federati vengono fornite credenziali di sicurezza temporanee per accedere AWS alle risorse tramite una richiesta. `AssumeRole`

Di seguito è riportato un evento di esempio per una richiesta di crittografia di federazione. L'ID della chiave di accesso originale viene fornito nel campo `accessKeyId` dell'elemento `userIdentity`. Il campo `accessKeyId` in `responseElements` contiene un nuovo ID della chiave di accesso se il `sessionDuration` richiesto viene passato nella richiesta di crittografia, altrimenti contiene il valore dell'ID della chiave di accesso originale.

> **Note**
>
> In questo esempio, il `mfaAuthenticated` valore è `false` e il `MFAUsed` valore è No perché la richiesta è stata effettuata da un utente federato. Questi campi verranno impostati su true solo se la richiesta è stata effettuata da un utente IAM o da un utente root che utilizza MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
```

```
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Di seguito viene illustrato un evento di accesso riuscito per un utente federato che non utilizza l'autenticazione a più fattori (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Lavorare con i file di CloudTrail registro

È possibile eseguire attività più avanzate con i CloudTrail file.

- Monitora i file di CloudTrail registro inviandoli a CloudWatch Logs.
- Condivisione dei file di log tra account.
- Utilizzate la AWS CloudTrail Processing Library per scrivere applicazioni di elaborazione dei log in Java.
- Convalida dei file di log per verificare la presenza di eventuali modifiche dopo la distribuzione da parte di CloudTrail.

Quando si verifica un evento nel tuo account, CloudTrail valuta se l'evento corrisponde alle impostazioni dei tuoi percorsi. Solo gli eventi che corrispondono alle impostazioni del percorso vengono inviati al bucket Amazon S3 e al gruppo di CloudWatch log Amazon Logs.

Puoi configurare più trail in modo tale che elaborino e registrino solo gli eventi specificati. Ad esempio, un trail può registrare gli eventi di dati e gli eventi di gestione di sola lettura in modo tale che tutti gli eventi di sola lettura vengano distribuiti in un bucket S3 specifico. Un altro trail può registrare gli eventi di dati e gli eventi di gestione di sola scrittura in modo tale che tutti gli eventi di sola scrittura vengano distribuiti in un bucket S3 distinto.

Puoi anche configurare i trail in modo che un trail registri e distribuisca tutti gli eventi di gestione in un bucket S3 e un altro trail registri e distribuisca tutti gli eventi di dati in un altro bucket S3.

Puoi configurare i trail per la registrazione dei seguenti eventi:

- Eventi di dati: questi eventi forniscono visibilità sulle operazioni eseguite in una risorsa o al suo interno. Queste operazioni sono definite anche operazioni del piano dei dati.
- Eventi di gestione: gli eventi di gestione forniscono visibilità sulle operazioni di gestione eseguite sulle risorse del tuo account. AWS Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Gli eventi di gestione possono includere anche eventi non API che si verificano nel tuo account. Ad esempio, quando un utente accede al tuo account, CloudTrail registra l'`ConsoleLogin`evento. Per ulteriori informazioni, consulta Eventi non API acquisiti da CloudTrail.
- Eventi di attività di CloudTrail rete: gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC

privato a. Servizio AWS Gli eventi di attività di rete forniscono visibilità sulle operazioni sulle risorse eseguite all'interno di un VPC.

- Eventi Insights: gli eventi Insights acquisiscono l'attività insolita rilevata nel tuo account. Se hai attivato gli eventi Insights e CloudTrail rileva attività insolite, gli eventi Insights vengono registrati nel bucket S3 di destinazione del percorso, ma in una cartella diversa. Puoi anche vedere il tipo di evento Insights e il periodo di tempo dell'incidente quando visualizzi gli eventi Insights sulla console. CloudTrail A differenza di altri tipi di eventi acquisiti in un CloudTrail trail, gli eventi di Insights vengono registrati solo quando CloudTrail rilevano cambiamenti nell'utilizzo dell'API dell'account che differiscono significativamente dai modelli di utilizzo tipici dell'account.

  Gli eventi Insights vengono generati solo per la gestione. APIs Per ulteriori informazioni, consulta Lavorare con CloudTrail Insights.

> **Note**
>
> CloudTrail in genere fornisce i log entro una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail.
> Se configuri male il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterai di recapitare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti ai costi standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Argomenti

- Ricezione di file di CloudTrail registro da più regioni
- Gestione della coerenza dei dati in CloudTrail
- Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs
- Ricezione di file di CloudTrail registro da più account
- Condivisione di file di CloudTrail registro tra AWS account
- Convalida dell'integrità dei file di CloudTrail registro
- CloudTrail esempi di file di registro
- Utilizzo della libreria CloudTrail di elaborazione

Ricezione di file di CloudTrail registro da più regioni

Quando crei un percorso multiregionale, CloudTrail registra gli eventi di tutte le regioni abilitate nel tuo account. CloudTrail invia i file di registro allo stesso bucket S3 e CloudWatch allo stesso gruppo di log Logs. Finché si CloudTrail dispone delle autorizzazioni di scrittura su un bucket S3, non è necessario che il bucket per un percorso multiregionale si trovi nella regione di origine del percorso.

Sebbene la Regioni AWS maggior parte sia abilitata di default per la tua Account AWS, devi abilitare manualmente alcune regioni (chiamate anche regioni opt-in). Per informazioni su quali regioni sono abilitate per impostazione predefinita, consulta Considerazioni prima di abilitare e disabilitare le regioni nella Gestione dell'account AWS Guida di riferimento. Per l'elenco delle regioni CloudTrail supportate, vedere. CloudTrail Regioni supportate

Dopo aver abilitato una regione opt-in, CloudTrail crea una copia identica di ogni percorso multiregionale nella regione opt-in che hai abilitato. Per ulteriori informazioni, consulta Cosa succede quando abiliti una regione opt-in?.

Se successivamente disattivi una regione con attivazione, la copia del percorso multiregionale in quella regione rimarrà. Poiché sul tuo account potrebbero essere presenti attività nella regione che hai disabilitato, ad esempio azioni volte Servizi AWS a rimuovere risorse, CloudTrail continuerà a registrare l'attività e tenterà di inviare eventi al bucket S3 per tutti i percorsi che non vengono eliminati prima della disattivazione della regione.

Per convertire un itinerario a regione singola esistente in un percorso multiregionale, è necessario utilizzare il. AWS CLI

Per modificare un itinerario esistente in modo che si applichi a tutte le regioni abilitate, aggiungete l'`--is-multi-region-trail`opzione al comando. update-trail

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Per confermare che l'itinerario è ora un percorso multiregionale, verificate che l'`IsMultiRegionTrail`elemento nell'output sia visualizzato`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
```

```
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Per ulteriori informazioni, consulta le seguenti risorse:

- Comprendere i percorsi multiregionali e le regioni opt-in
- Creare un percorso per il tuo Account AWS
- CloudTrail FAQs

Gestione della coerenza dei dati in CloudTrail

CloudTrail utilizza un modello di calcolo distribuito chiamato coerenza finale. Qualsiasi modifica apportata alla CloudTrail configurazione (o ad altri AWS servizi), compresi i tag utilizzati nel controllo degli accessi basato sugli attributi (ABAC), richiede tempo per diventare visibile da tutti gli endpoint possibili. Parte del ritardo deriva dal tempo necessario per inviare i dati da un server all'altro e da una regione all'altra in tutto il mondo. CloudTrail utilizza anche la memorizzazione nella cache per migliorare le prestazioni, ma in alcuni casi ciò può comportare un aumento di tempo. in quanto la modifica potrebbe risultare visibile solo dopo il timeout dei dati memorizzati nella cache.

È necessario progettare le applicazioni in modo da tenere in considerazione questi potenziali ritardi e assicurarsi che funzionino come previsto, anche quando una modifica apportata in una posizione non è immediatamente visibile in un'altra. Tali modifiche includono l'attivazione di una regione di attivazione, la creazione o l'aggiornamento di percorsi o archivi di dati di eventi, l'aggiornamento dei selettori di eventi e l'avvio o l'interruzione della registrazione. Quando crei o aggiorni un archivio dati di percorsi o eventi, CloudTrail invia i log al bucket S3 o al data store degli eventi in base all'ultima configurazione nota fino a quando le modifiche non si propagano in tutte le posizioni.

Per ulteriori informazioni su come ciò influisce sugli altri Servizi AWS, consulta le seguenti risorse:

- Amazon DynamoDB: Cos'è il modello di consistenza di DynamoDB? nelle Domande frequenti su DynamoDB e Read consistency (Coerenza di lettura) nella Guida per gli sviluppatori di Amazon DynamoDB.
- Amazon EC2: coerenza finale nell'Amazon Elastic Compute Cloud API Reference.
- Amazon EMR: garantire la coerenza nell'utilizzo di Amazon S3 e MapReduce Amazon Elastic for ETL Workflows AWS nel blog sui Big Data.

- AWS Identity and Access Management (IAM): Le modifiche che apporto non sono sempre immediatamente visibili nella IAM User Guide.
- Amazon Redshift: Managing data consistency (Gestione della coerenza dei dati) nella Guida per gli sviluppatori di Amazon Redshift Database.
- Amazon S3: Amazon S3 data consistency model (Modello di consistenza dei dati di Amazon S3) nella Guida per l'utente di Amazon Simple Storage Service.

Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs

Puoi utilizzare Amazon CloudWatch Logs per monitorare, archiviare e accedere ai tuoi file di registro da CloudTrail.

CloudWatch Logs ti consente di centralizzare i log di tutti i tuoi sistemi, applicazioni e quelli Servizi AWS che utilizzi, in un unico servizio altamente scalabile. Potrai quindi visualizzarli facilmente, cercarli per codici o modelli di errore specifici, filtrarli in base a campi specifici o archiviarli in modo sicuro per analisi future. CloudWatch I registri consentono di visualizzare tutti i registri, indipendentemente dalla loro origine, come un flusso unico e coerente di eventi ordinati per ora.

Completa i seguenti passaggi per configurare CloudTrail CloudWatch Logs per monitorare i log dei percorsi e ricevere notifiche quando si verifica un'attività specifica.

1. Configura il percorso per inviare gli eventi di registro ai CloudWatch registri.
2. Definisci i filtri metrici di CloudWatch Logs per valutare gli eventi di registro per verificare le corrispondenze in termini, frasi o valori. Ad esempio, puoi monitorare gli eventi `ConsoleLogin`.
3. Assegna le metriche ai CloudWatch filtri metrici.
4. Crea CloudWatch allarmi che vengono attivati in base alle soglie e ai periodi di tempo specificati. È possibile configurare gli allarmi per l'invio di notifiche quando gli allarmi vengono attivati, in modo da poter intervenire tempestivamente.
5. Puoi anche configurare l'esecuzione automatica CloudWatch di un'azione in risposta a un allarme.

Si applicano i prezzi standard per Amazon CloudWatch e Amazon CloudWatch Logs. Per ulteriori informazioni, consulta la pagina CloudWatch dei prezzi di Amazon.

Per ulteriori informazioni sulle regioni in cui puoi configurare i percorsi per inviare log a Logs, consulta Amazon CloudWatch CloudWatch Logs Regions and Quotas nel General Reference.AWS

Argomenti

- Invio di eventi ai registri CloudWatch
- Creazione CloudWatch di allarmi per CloudTrail eventi: esempi
- Interruzione dell'invio CloudTrail di eventi ai registri CloudWatch
- CloudWatch denominazione dei gruppi di log e dei flussi di log per CloudTrail
- Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio

Invio di eventi ai registri CloudWatch

Quando configuri il percorso per inviare eventi ai CloudWatch registri, CloudTrail invia solo gli eventi che corrispondono alle impostazioni del percorso. Ad esempio, se configuri il percorso per registrare solo gli eventi relativi ai dati, il percorso invia gli eventi relativi ai dati solo al gruppo di log CloudWatch Logs. CloudTrail supporta l'invio di dati, Insights ed eventi di gestione a CloudWatch Logs. Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro.

> **Note**
>
> Solo l'account di gestione può configurare un gruppo di log CloudWatch Logs per un percorso organizzativo utilizzando la console. L'amministratore delegato può configurare un gruppo di log CloudWatch Logs utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API.

Per inviare eventi a un gruppo di CloudWatch log Logs:

- Verifica di disporre di autorizzazioni sufficienti per creare o specificare un ruolo IAM. Per ulteriori informazioni, consulta Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail .
- Se stai configurando il gruppo di log CloudWatch Logs utilizzando il AWS CLI, assicurati di disporre delle autorizzazioni sufficienti per creare un flusso di log CloudWatch Logs nel gruppo di log specificato e per inviare CloudTrail eventi a quel flusso di log. Per ulteriori informazioni, consulta Creazione di un documento di policy.

- Creare un nuovo trail oppure specificarne uno esistente. Per ulteriori informazioni, consulta Creazione e aggiornamento di un percorso con la console.
- Crea un gruppo di log oppure specificane uno esistente.
- Specifica un ruolo IAM. Se modifichi un ruolo IAM esistente per un percorso dell'organizzazione, devi aggiornare manualmente la policy per permettere la registrazione per il percorso dell'organizzazione. Per ulteriori informazioni, consulta questo esempio di policy e Creazione di un percorso per un'organizzazione.
- Collegare una policy di ruolo oppure usare una policy di default.

Indice

- Configurazione del monitoraggio dei log con la console CloudWatch
  - Creazione di un gruppo di log o indicazione di un gruppo di log esistente
  - Specificare un ruolo IAM
  - Visualizzazione degli eventi nella console CloudWatch
- Configurazione del monitoraggio CloudWatch dei registri con AWS CLI
  - Creazione di un gruppo di log
  - Creazione di un ruolo
  - Creazione di un documento di policy
  - Aggiornamento del percorso
- Limitazione

Configurazione del monitoraggio dei log con la console CloudWatch

Puoi usare il AWS Management Console per configurare il tuo percorso per inviare eventi a CloudWatch Logs per il monitoraggio.

Creazione di un gruppo di log o indicazione di un gruppo di log esistente

CloudTrail utilizza un gruppo di log CloudWatch Logs come endpoint di consegna per gli eventi di registro. Puoi creare un gruppo di log oppure specificarne uno esistente.

Creazione o specifica di un gruppo di log per un percorso esistente

1. Assicurati di accedere con un utente o un ruolo amministrativo con autorizzazioni sufficienti per configurare CloudWatch l'integrazione di Logs. Per ulteriori informazioni, consulta Concessione

dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail .

> **Note**
>
> Solo l'account di gestione può configurare un gruppo di log CloudWatch Logs per un percorso organizzativo utilizzando la console. L'amministratore delegato può configurare un gruppo di log CloudWatch Logs utilizzando le operazioni AWS CLI or CloudTrail `CreateTrail` o `UpdateTrail` API.

2. Apri la CloudTrail console all'indirizzo. https://console.aws.amazon.com/cloudtrail/
3. Scegliere il nome del trail. Se scegli un percorso multiregionale, verrai reindirizzato alla regione in cui è stato creato il percorso. Puoi creare un gruppo di log o sceglierne uno esistente nella stessa Regione del percorso.

> **Note**
>
> Un percorso multiregionale invia i file di registro da tutte le regioni abilitate dell'utente Account AWS al gruppo di log CloudWatch Logs specificato.

4. In CloudWatch Registri, scegli Modifica.
5. Per CloudWatch Registri, scegli Abilitato.
6. Per Nome del gruppo di log, scegli Nuovo per creare un nuovo gruppo di log o Esistente per utilizzarne uno esistente. Se scegli Nuovo, CloudTrail specifica automaticamente un nome per il nuovo gruppo di log oppure puoi digitare un nome. Per ulteriori informazioni sulla denominazione, consulta CloudWatch denominazione dei gruppi di log e dei flussi di log per CloudTrail.
7. Se scegli Existing (Esistente), seleziona un gruppo di log dall'elenco a discesa.
8. Per Nome del ruolo, scegli Nuovo per creare un nuovo ruolo IAM per le autorizzazioni all'invio dei log ai registri. CloudWatch Scegli Existing (Esistente) per selezionare un ruolo IAM esistente dall'elenco a discesa. L'istruzione della policy per il ruolo nuovo o esistente viene visualizzata quando espandi Policy document (Documento della policy). Per ulteriori informazioni su questo ruolo, consulta Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio.

> **Note**
>
> Durante la configurazione di un percorso, puoi scegliere un bucket S3 e un argomento SNS appartenenti a un altro account. Tuttavia, se desideri inviare eventi CloudTrail a un gruppo di log CloudWatch Logs, devi scegliere un gruppo di log esistente nel tuo account corrente.

9. Scegli Save changes (Salva modifiche).

Specificare un ruolo IAM

È possibile specificare un ruolo CloudTrail da assumere per fornire eventi al flusso di log.

Per specificare un ruolo

1. Per impostazione di default, il ruolo `CloudTrail_CloudWatchLogs_Role` viene specificato automaticamente. La politica di ruolo predefinita dispone delle autorizzazioni necessarie per creare un flusso di log di CloudWatch Logs in un gruppo di log specificato dall'utente e per inviare CloudTrail eventi a quel flusso di log.

   > **Note**
   >
   > Se vuoi utilizzare questo ruolo per un gruppo di log per un trail dell'organizzazione, devi modificare manualmente la policy dopo aver creato il ruolo. Per ulteriori informazioni, consulta questo esempio di policy e Creazione di un percorso per un'organizzazione.

   a. Per verificare il ruolo, accedi alla AWS Identity and Access Management console all'indirizzo. https://console.aws.amazon.com/iam/
   b. Scegli Ruoli, quindi scegli CloudTrail_ CloudWatchLogs _Ruolo.
   c. Dalla scheda Autorizzazioni, espandi la policy per visualizzarne il contenuto.
2. È possibile specificare un altro ruolo, ma è necessario allegare la politica del ruolo richiesta al ruolo esistente se si desidera utilizzarla per inviare eventi ai CloudWatch registri. Per ulteriori informazioni, consulta Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio.

Visualizzazione degli eventi nella console CloudWatch

Dopo aver configurato il percorso per inviare eventi al gruppo di log CloudWatch Logs, puoi visualizzare gli eventi nella CloudWatch console. CloudTrail in genere invia gli eventi al gruppo di log entro una media di circa 5 minuti da una chiamata API. Questo tempo non è garantito. Per ulteriori informazioni, consultare l'Accordo sul Livello di Servizio (SLA) di AWS CloudTrail.

Per visualizzare gli eventi nella CloudWatch console

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione sulla sinistra, in Log, scegli Gruppi di log.
3. Scegliere il gruppo di log specificato per il trail.
4. Scegli il flusso di log da visualizzare.
5. Per visualizzare i dettagli dell'evento registrato dal trail, scegliere un evento.

> **Note**
>
> La colonna Time (UTC) nella CloudWatch console mostra quando l'evento è stato consegnato al tuo gruppo di log. Per vedere l'ora effettiva in cui l'evento è stato registrato CloudTrail, consulta il `eventTime` campo.

Configurazione del monitoraggio CloudWatch dei registri con AWS CLI

È possibile utilizzare AWS CLI to configure per inviare eventi CloudTrail a CloudWatch Logs per il monitoraggio.

Creazione di un gruppo di log

1. Se non disponi di un gruppo di log esistente, crea un gruppo di log CloudWatch Logs come endpoint di consegna per gli eventi di registro utilizzando il comando CloudWatch `create-log-group` Logs.

   ```
   aws logs create-log-group --log-group-name name
   ```

   Nell'esempio seguente viene creato un gruppo di log denominato `CloudTrail/logs`:

```
aws logs create-log-group --log-group-name CloudTrail/logs
```

2. Recuperare l'ARN (Amazon Resource Name) del gruppo di log.

```
aws logs describe-log-groups
```

Creazione di un ruolo

Crea un ruolo CloudTrail che gli consenta di inviare eventi al gruppo di CloudWatch log Logs. Il comando IAM `create-role` accetta due parametri: un nome di ruolo e un percorso di file di un documento di policy di ruolo in formato JSON. Il documento di policy che utilizzi fornisce `AssumeRole` le autorizzazioni a. CloudTrail Il comando `create-role` crea il ruolo con le autorizzazioni richieste.

Per creare il file JSON che conterrà il documento di policy, apri un editor di testo e salva i seguenti contenuti delle policy in un file denominato `assume_role_policy_document.json`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Esegui il comando seguente per creare il ruolo con le `AssumeRole` autorizzazioni per. CloudTrail

```
aws iam create-role --role-name role_name --assume-role-policy-document file:///<path to
 assume_role_policy_document>.json
```

Quando il comando viene completato, annota l'ARN del ruolo nell'output.

Creazione di un documento di policy

Crea il seguente documento sulla politica dei ruoli per CloudTrail. Questo documento concede CloudTrail le autorizzazioni necessarie per creare un flusso di log di CloudWatch Logs nel gruppo di log specificato e per inviare CloudTrail eventi a tale flusso di log.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        }
    ]
}
```

Salva il documento di policy in un file denominato `role-policy-document.json`.

Se stai creando una policy che potrebbe essere utilizzata anche per il trail dell'organizzazione, dovrai configurarlo in modo leggermente diverso. Ad esempio, la seguente politica concede CloudTrail le autorizzazioni necessarie per creare un flusso di log di CloudWatch Logs nel gruppo di log specificato e per inviare CloudTrail eventi a quel flusso di log per entrambi i percorsi nell' AWS account 1111 e per gli itinerari organizzativi creati nell'account 1111 che vengono applicati all'organizzazione con l'ID di: AWS Organizations *o-exampleorgid*

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-aa111bb222_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-aa111bb222_*"
            ]
        }
    ]
}
```

Per ulteriori informazioni sui trail dell'organizzazione, consulta Creazione di un percorso per un'organizzazione.

Esegui il seguente comando per applicare la policy al ruolo.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

Aggiornamento del percorso

Aggiorna il percorso con il gruppo di log e le informazioni sul ruolo utilizzando il comando. CloudTrail `update-trail`

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Per ulteriori informazioni sui AWS CLI comandi, consulta il AWS CloudTrail Command Line Reference.

Limitazione

CloudWatch EventBridge Ciascuno dei log consente una dimensione massima degli eventi di 256 KB. Sebbene la maggior parte degli eventi di servizio abbia una dimensione massima di 256 KB, alcuni servizi presentano ancora eventi più grandi. CloudTrail non invia questi eventi a CloudWatch Logs o EventBridge.

A partire CloudTrail dalla versione 1.05, gli eventi hanno una dimensione massima di 256 KB. Questo serve a prevenire lo sfruttamento da parte di malintenzionati e a consentire la fruizione degli eventi da parte di altri AWS servizi, come CloudWatch Logs e. EventBridge

Creazione CloudWatch di allarmi per CloudTrail eventi: esempi

Questo argomento descrive come configurare gli allarmi per CloudTrail gli eventi e include esempi.

Argomenti

- Prerequisiti
- Creazione di un filtro parametri e creazione di un allarme
- Esempio di modifiche della configurazione del gruppo di sicurezza
- Esempi di errori di AWS Management Console accesso

- Esempio: modifiche delle policy IAM
- Configurazione delle notifiche per CloudWatch Logs (allarmi)

Prerequisiti

Prima di utilizzare gli esempi di questo argomento, è necessario:

- Creare un trail con la console o l'interfaccia a riga di comando (CLI).
- Crea un gruppo di log, operazione che puoi eseguire durante la creazione di un percorso. Per ulteriori informazioni sulla creazione di un trail, consulta Creazione di un percorso con la CloudTrail console.
- Specificate o create un ruolo IAM che conceda CloudTrail le autorizzazioni per creare un flusso di log CloudWatch Logs nel gruppo di log specificato e per inviare CloudTrail eventi a quel flusso di log. L'impostazione di default `CloudTrail_CloudWatchLogs_Role` è valida per questo esempio.

Per ulteriori informazioni, consulta Invio di eventi ai registri CloudWatch . Gli esempi in questa sezione vengono eseguiti nella console Amazon CloudWatch Logs. Per ulteriori informazioni su come creare filtri metrici e allarmi, consulta Creazione di metriche da eventi di registro utilizzando filtri e Uso degli CloudWatch allarmi Amazon nella Amazon User Guide. CloudWatch

Creazione di un filtro parametri e creazione di un allarme

Per creare un allarme, devi prima creare un filtro dei parametri e quindi configurare un allarme in base a tale filtro. Le procedure vengono riportate per tutti gli esempi. Per ulteriori informazioni sulla sintassi dei filtri metrici e dei modelli per gli eventi di CloudTrail log, consulta le sezioni relative a JSON della sintassi dei filtri e dei pattern nella Amazon Logs User Guide. CloudWatch

Esempio di modifiche della configurazione del gruppo di sicurezza

Segui questa procedura per creare un CloudWatch allarme Amazon che viene attivato quando si verificano modifiche alla configurazione nei gruppi di sicurezza.

Creazione di un filtro parametri

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, in Log, scegli Gruppi di log.
3. Nell'elenco dei gruppi di log, scegli il gruppo di log creato per il percorso.

4. Dal menu Filtri parametri o Operazioni, scegli Crea filtro parametri.
5. Nella pagina Define pattern (Definisci il modello), in Create filter pattern (Crea un modello di filtro), inserisci i seguenti dati per Filter pattern (Modello di filtro).

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. In Test pattern (Modello di test), lascia le impostazioni predefinite. Scegli Next (Successivo).
7. Nella pagina Assegna parametro, per Nome filtro inserisci **`SecurityGroupEvents`**.
8. In Dettagli parametro attiva Crea nuovo e quindi inserisci **`CloudTrailMetrics`** per Spazio nomi parametro.
9. Per Nome parametro digita **`SecurityGroupEventCount`**.
10. Per Valore parametro, digita **`1`**.
11. Lascia vuoto il campo Default value (Valore predefinito).
12. Scegli Next (Successivo).
13. Nella pagina Review and create (Rivedi e crea), esamina le opzioni selezionate. Scegli Create metric filter (Crea filtro parametri) per creare il filtro, oppure scegli Edit (Modifica) per tornare indietro e modificare i valori.

Creazione di un allarme

Dopo aver creato il filtro metrico, si apre la pagina dei dettagli del gruppo di CloudWatch log dei log dei log dei CloudTrail percorsi. Segui questa procedura per creare un allarme.

1. Nella scheda Metric filters (Filtri parametri), trovare il filtro del parametro creato in the section called “Creazione di un filtro parametri”. Compila la casella di controllo del filtro del parametro. Nella barra Metric filters (Filtri parametri), scegli Create alarm (Crea allarme).
2. Per Specifica parametri e condizioni, inserisci quanto segue.
   a. Per Graph (Grafico), la riga è impostata su **`1`** in base alle altre impostazioni che selezioni quando crei l'allarme.
   b. PerMetric name (Nome parametro), mantieni il nome del parametro corrente, **`SecurityGroupEventCount`**.
   c. Per Statistic (Statistica), mantieni l'impostazione predefinita, **`Sum`**.

   d. Per Period (Periodo), mantieni l'impostazione predefinita, **`5 minutes`**.
   e. In Conditions (Condizioni), per Threshold type (Tipo di soglia) scegli Static (Statica).
   f. Per Whenever ***`metric_name`*** is, scegli Greater/Equal.
   g. Per il valore di soglia, immetti **`1`**.
   h. In Additional configuration (Configurazione aggiuntiva), lascia le impostazioni predefinite. Scegli Next (Successivo).
3. Nella pagina Configura azioni, scegli Notifica, quindi scegli In allarme, il che indica che l'azione viene intrapresa quando viene superata la soglia di 1 evento di modifica in 5 minuti e si SecurityGroupEventCounttrova in uno stato di allarme.
   a. Nella sezione Invia una notifica al seguente argomento SNS, scegli Crea un nuovo argomento.
   b. Immetti **`SecurityGroupChanges_CloudWatch_Alarms_Topic`** come nome per il nuovo argomento Amazon SNS.
   c. In Endpoint delle e-mail che riceveranno la notifica inserisci gli indirizzi e-mail degli utenti che vuoi che ricevano notifiche se viene generato questo allarme. Separa gli indirizzi e-mail con virgole.

      Ogni destinatario e-mail riceverà un'e-mail che chiede di confermare che vogliono effettuare la sottoscrizione all'argomento Amazon SNS.
   d. Scegli Create topic (Crea argomento).
4. Per questo esempio, ignora gli altri tipi di azione. Scegli Next (Successivo).
5. Nella pagina Add name and description (Aggiungi nome e descrizione) inserisci un nome descrittivo per l'allarme e una descrizione. In questo esempio, inserisci **`Security group configuration changes`** per il nome e **`Raises alarms if security group configuration changes occur`** per la descrizione. Scegli Next (Successivo).
6. Nella pagina Review and create (Anteprima e creazione), esamina le opzioni selezionate. Scegli Edit (Modifica) per apportare modifiche o scegli Create alarm (Crea allarme) per creare l'allarme.

   Dopo aver creato l'allarme, CloudWatch apre la pagina Allarmi. La colonna Actions (Operazioni) dell'allarme mostra Pending confirmation (In attesa di conferma) fino a quando tutti i destinatari dell'e-mail sull'argomento SNS hanno confermato di voler effettuare la sottoscrizione alle notifiche SNS.

Esempi di errori di AWS Management Console accesso

Segui questa procedura per creare un CloudWatch allarme Amazon che si attiva quando si verificano tre o più errori di AWS Management Console accesso in un periodo di cinque minuti.

Creazione di un filtro parametri

1. Apri la console all' CloudWatch indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel pannello di navigazione, in Log, scegli Gruppi di log.
3. Nell'elenco dei gruppi di log, scegli il gruppo di log creato per il percorso.
4. Dal menu Filtri parametri o Operazioni, scegli Crea filtro parametri.
5. Nella pagina Define pattern (Definisci il modello), in Create filter pattern (Crea un modello di filtro), inserisci i seguenti dati per Filter pattern (Modello di filtro).

   ```
   { ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
   ```

6. In Test pattern (Modello di test), lascia le impostazioni predefinite. Scegli Next (Successivo).
7. Nella pagina Assegna parametro, per Nome filtro inserisci **`ConsoleSignInFailures`**.
8. In Dettagli parametro attiva Crea nuovo e quindi inserisci **`CloudTrailMetrics`** per Spazio nomi parametro.
9. Per Nome parametro digita **`ConsoleSigninFailureCount`**.
10. Per Valore parametro, digita **`1`**.
11. Lascia vuoto il campo Default value (Valore predefinito).
12. Scegli Next (Successivo).
13. Nella pagina Review and create (Rivedi e crea), esamina le opzioni selezionate. Scegli Create metric filter (Crea filtro parametri) per creare il filtro, oppure scegli Edit (Modifica) per tornare indietro e modificare i valori.

Creazione di un allarme

Dopo aver creato il filtro metrico, si apre la pagina dei dettagli del gruppo di CloudWatch log dei log dei log dei CloudTrail percorsi. Segui questa procedura per creare un allarme.

1. Nella scheda Metric filters (Filtri parametri), trovare il filtro del parametro creato in the section called “Creazione di un filtro parametri”. Compila la casella di controllo del filtro del parametro. Nella barra Metric filters (Filtri parametri), scegli Create alarm (Crea allarme).

2. Nella pagina Create alarm (Crea allarme), in Specify metric and conditions (Specifica parametri e condizioni), inserisci i seguenti dati.

   a. Per Graph (Grafico), la riga è impostata su **3** in base alle altre impostazioni che selezioni quando crei l'allarme.

   b. PerMetric name (Nome parametro), mantieni il nome del parametro corrente, **`ConsoleSigninFailureCount`**.

   c. Per Statistic (Statistica), mantieni l'impostazione predefinita, **`Sum`**.

   d. Per Period (Periodo), mantieni l'impostazione predefinita, **`5 minutes`**.

   e. In Conditions (Condizioni), per Threshold type (Tipo di soglia) scegli Static (Statica).

   f. Per Whenever ***`metric_name`*** is, scegli Greater/Equal.

   g. Per il valore di soglia, immetti **`3`**.

   h. In Additional configuration (Configurazione aggiuntiva), lascia le impostazioni predefinite. Scegli Next (Successivo).

3. Nella pagina Configura azioni, per Notifica, scegli In allarme, che indica che l'azione viene intrapresa quando viene superata la soglia di 3 eventi di modifica in 5 minuti e si ConsoleSigninFailureCounttrova in uno stato di allarme.

   a. Nella sezione Invia una notifica al seguente argomento SNS, scegli Crea un nuovo argomento.

   b. Immetti **`ConsoleSignInFailures_CloudWatch_Alarms_Topic`** come nome per il nuovo argomento Amazon SNS.

   c. In Endpoint delle e-mail che riceveranno la notifica inserisci gli indirizzi e-mail degli utenti che vuoi che ricevano notifiche se viene generato questo allarme. Separa gli indirizzi e-mail con virgole.

      Ogni destinatario e-mail riceverà un'e-mail che chiede di confermare che vogliono effettuare la sottoscrizione all'argomento Amazon SNS.

   d. Scegli Create topic (Crea argomento).

4. Per questo esempio, ignora gli altri tipi di azione. Scegli Next (Successivo).

5. Nella pagina Add name and description (Aggiungi nome e descrizione) inserisci un nome descrittivo per l'allarme e una descrizione. In questo esempio, inserisci **`Console sign-in failures`** per il nome e **`Raises alarms if more than 3 console sign-in failures occur in 5 minutes`** per la descrizione. Scegli Next (Successivo).

6. Nella pagina Review and create (Anteprima e creazione), esamina le opzioni selezionate. Scegli Edit (Modifica) per apportare modifiche o scegli Create alarm (Crea allarme) per creare l'allarme.

   Dopo aver creato l'allarme, CloudWatch apre la pagina Allarmi. La colonna Actions (Operazioni) dell'allarme mostra Pending confirmation (In attesa di conferma) fino a quando tutti i destinatari dell'e-mail sull'argomento SNS hanno confermato di voler effettuare la sottoscrizione alle notifiche SNS.

Esempio: modifiche delle policy IAM

Segui questa procedura per creare un CloudWatch allarme Amazon che viene attivato quando viene effettuata una chiamata API per modificare una policy IAM.

Creazione di un filtro parametri

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione scegli Logs (Log).
3. Nell'elenco dei gruppi di log, scegli il gruppo di log creato per il percorso.
4. Scegli Actions (Operazioni) e quindi Create metric filter (Crea filtro parametri).
5. Nella pagina Define pattern (Definisci il modello), in Create filter pattern (Crea un modello di filtro), inserisci i seguenti dati per Filter pattern (Modello di filtro).

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. In Test pattern (Modello di test), lascia le impostazioni predefinite. Scegli Next (Successivo).
7. Nella pagina Assegna parametro, per Nome filtro inserisci **`IAMPolicyChanges`**.
8. In Dettagli parametro attiva Crea nuovo e quindi inserisci **`CloudTrailMetrics`** per Spazio nomi parametro.
9. Per Nome parametro digita **`IAMPolicyEventCount`**.
10. Per Valore parametro, digita **`1`**.

11. Lascia vuoto il campo Default value (Valore predefinito).
12. Scegli Next (Successivo).
13. Nella pagina Review and create (Rivedi e crea), esamina le opzioni selezionate. Scegli Create metric filter (Crea filtro parametri) per creare il filtro, oppure scegli Edit (Modifica) per tornare indietro e modificare i valori.

Creazione di un allarme

Dopo aver creato il filtro metrico, si apre la pagina dei dettagli del gruppo di CloudWatch log dei log dei log dei CloudTrail percorsi. Segui questa procedura per creare un allarme.

1. Nella scheda Metric filters (Filtri parametri), trovare il filtro del parametro creato in the section called “Creazione di un filtro parametri”. Compila la casella di controllo del filtro del parametro. Nella barra Metric filters (Filtri parametri), scegli Create alarm (Crea allarme).
2. Nella pagina Create alarm (Crea allarme), in Specify metric and conditions (Specifica parametri e condizioni), inserisci i seguenti dati.
   a. Per Graph (Grafico), la riga è impostata su **`1`** in base alle altre impostazioni che selezioni quando crei l'allarme.
   b. PerMetric name (Nome parametro), mantieni il nome del parametro corrente, **`IAMPolicyEventCount`**.
   c. Per Statistic (Statistica), mantieni l'impostazione predefinita, **`Sum`**.
   d. Per Period (Periodo), mantieni l'impostazione predefinita, **`5 minutes`**.
   e. In Conditions (Condizioni), per Threshold type (Tipo di soglia) scegli Static (Statica).
   f. Per Whenever ***`metric_name`*** is, scegli Greater/Equal.
   g. Per il valore di soglia, immetti **`1`**.
   h. In Additional configuration (Configurazione aggiuntiva), lascia le impostazioni predefinite. Scegli Next (Successivo).
   i.
3. Nella pagina Configura azioni, per Notifica, scegli In allarme, che indica che l'azione viene intrapresa quando viene superata la soglia di 1 evento di modifica in 5 minuti e si IAMPolicyEventCounttrova in uno stato di allarme.
   a. Nella sezione Invia una notifica al seguente argomento SNS, scegli Crea un nuovo argomento.

b. Immetti **`IAM_Policy_Changes_CloudWatch_Alarms_Topic`** come nome per il nuovo argomento Amazon SNS.

c. In Endpoint delle e-mail che riceveranno la notifica inserisci gli indirizzi e-mail degli utenti che vuoi che ricevano notifiche se viene generato questo allarme. Separa gli indirizzi e-mail con virgole.

   Ogni destinatario e-mail riceverà un'e-mail che chiede di confermare che vogliono effettuare la sottoscrizione all'argomento Amazon SNS.

d. Scegli Create topic (Crea argomento).

4. Per questo esempio, ignora gli altri tipi di azione. Scegli Next (Successivo).
5. Nella pagina Add name and description (Aggiungi nome e descrizione) inserisci un nome descrittivo per l'allarme e una descrizione. In questo esempio, inserisci **`IAM Policy Changes`** per il nome e **`Raises alarms if IAM policy changes occur`** per la descrizione. Scegli Next (Successivo).
6. Nella pagina Review and create (Anteprima e creazione), esamina le opzioni selezionate. Scegli Edit (Modifica) per apportare modifiche o scegli Create alarm (Crea allarme) per creare l'allarme.

   Dopo aver creato l'allarme, CloudWatch apre la pagina Allarmi. La colonna Actions (Operazioni) dell'allarme mostra Pending confirmation (In attesa di conferma) fino a quando tutti i destinatari dell'e-mail sull'argomento SNS hanno confermato di voler effettuare la sottoscrizione alle notifiche SNS.

Configurazione delle notifiche per CloudWatch Logs (allarmi)

È possibile configurare CloudWatch Logs per inviare una notifica ogni volta che viene attivato un allarme. CloudTrail In questo modo è possibile rispondere rapidamente agli eventi operativi critici acquisiti negli CloudTrail eventi e rilevati da CloudWatch Logs. CloudWatch utilizza Amazon Simple Notification Service (SNS) per inviare e-mail. Per ulteriori informazioni, consulta Configurazione delle notifiche di Amazon SNS nella Guida per l'CloudWatch utente.

Interruzione dell'invio CloudTrail di eventi ai registri CloudWatch

Puoi interrompere l'invio di AWS CloudTrail eventi ad Amazon CloudWatch Logs aggiornando un percorso per disabilitare le impostazioni di CloudWatch Logs.

Interrompi l'invio di eventi a CloudWatch Logs (console)

Per interrompere l'invio di CloudTrail eventi ai registri CloudWatch

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Nel riquadro di navigazione selezionare Trails (Percorso).
3. Scegli il nome del percorso per il quale desideri disabilitare l'integrazione con CloudWatch Logs.
4. In CloudWatch Logs, scegli Modifica.
5. Deseleziona la casella Attivato.
6. Scegli Save changes (Salva modifiche).

Interrompi l'invio di eventi ai CloudWatch registri (CLI)

È possibile rimuovere il gruppo di log CloudWatch Logs come endpoint di consegna eseguendo il comando. update-trail Il comando seguente cancella il gruppo di log e il ruolo dalla configurazione trail sostituendo i valori per il gruppo di log ARN CloudWatch e Logs role ARN con valori vuoti.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch denominazione dei gruppi di log e dei flussi di log per CloudTrail

Amazon CloudWatch mostrerà il gruppo di log che hai creato per CloudTrail gli eventi insieme a tutti gli altri gruppi di log presenti in una regione. È consigliabile utilizzare un nome di gruppo di log che consenta di distinguere facilmente il gruppo di log dagli altri. Ad esempio **`CloudTrail/logs`**.

Segui queste linee guida quando scegli il nome di un gruppo di log:

- I nomi dei gruppi di log devono essere univoci in una regione per un Account AWS.
- I nomi dei gruppi di log possono essere lunghi da 1 a 512 caratteri.
- I nomi dei gruppi di log sono composti dai seguenti caratteri: a-z, A-Z, 0-9, "_" (sottolineatura), "-" (trattino), "/" (barra), "." (punto) e "#" (segno numerico).

Quando CloudTrail crea il flusso di log per il gruppo di log, nomina il flusso di log in base al seguente formato: *`account_ID`* _ CloudTrail _*`trail_region`*.

> **Note**
>
> Se il volume dei CloudTrail log è elevato, è possibile creare più flussi di log per fornire i dati di log al gruppo di log. Quando sono presenti più flussi di log, assegna un CloudTrail nome a ciascun flusso di log in base al seguente formato: *account_ID* _ _ _CloudTrail. *trail_region number*

Per ulteriori informazioni sui gruppi di CloudWatch log, consulta Working with log groups and log stream nella Amazon CloudWatch Logs User Guide e CreateLogGroupnell'Amazon CloudWatch Logs API Reference.

Documento sulla politica dei ruoli CloudTrail per l'utilizzo di CloudWatch Logs per il monitoraggio

Questa sezione descrive la politica di autorizzazione richiesta al CloudTrail ruolo per inviare eventi di registro a Logs. CloudWatch È possibile allegare un documento di policy a un ruolo quando si configura l'invio CloudTrail di eventi, come descritto in. Invio di eventi ai registri CloudWatch Puoi creare un ruolo anche utilizzando IAM. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un ruolo IAM Servizio AWS o Creazione di un ruolo IAM ()AWS CLI.

Il seguente documento politico di esempio contiene le autorizzazioni necessarie per creare un flusso di CloudWatch log nel gruppo di log specificato e per inviare CloudTrail eventi a quel flusso di log nella regione Stati Uniti orientali (Ohio). Questa è l'impostazione di default per il ruolo IAM `CloudTrail_CloudWatchLogs_Role`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
```

```
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        }
    ]
}
```

Se stai creando una policy che potrebbe essere utilizzata anche per i trail dell'organizzazione, dovrai modificarla a partire dalla policy predefinita creata per il ruolo. Ad esempio, la seguente politica concede CloudTrail le autorizzazioni necessarie per creare un flusso di log di CloudWatch Logs nel gruppo di *log_group_name* log specificato come valore e per inviare CloudTrail eventi a quel flusso di log per entrambi i trail nell' AWS account 1111 e per gli itinerari organizzativi creati nell'account 1111 che vengono applicati all' AWS Organizations organizzazione con l'ID di*o-exampleorgid*:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:o-exampleorgid_*"
```

```
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Per ulteriori informazioni sui trail dell'organizzazione, consulta Creazione di un percorso per un'organizzazione.

Ricezione di file di CloudTrail registro da più account

È possibile CloudTrail distribuire file di log da più bucket Amazon S3 Account AWS in un unico bucket Amazon S3. Ad esempio, ne hai quattro Account AWS con account IDs 1111, 222222222222, 3333 e 444444444444 e desideri configurare per consegnare i file di registro da tutti e quattro questi account CloudTrail a un bucket appartenente all'account 1111. Per eseguire questa operazione, completa i seguenti passaggi nell'ordine indicato:

1. Attiva un percorso nell'account a cui apparterrà il bucket di destinazione (111111111111, in questo esempio). Per il momento non creare un percorso per altri account.

   Per istruzioni, consultare Creazione di un percorso con la console.
2. Aggiornare la policy di bucket nel bucket di destinazione per concedere a CloudTrail le autorizzazioni tra più account.

   Per istruzioni, consultare Impostazione della policy del bucket per più account.
3. Crea un percorso negli altri account (222222222222, 333333333333 e 444444444444 in questo esempio) per cui desideri registrare l'attività. Quando crei il percorso in ogni account, specifica lo

stesso bucket Amazon S3 appartenente all'account specificato nel passaggio 1 (111111111111 in questo esempio). Per istruzioni, consultare Creazione di percorsi in account aggiuntivi.

> **Note**
>
> Se scegli di abilitare la crittografia SSE-KMS, la politica della chiave KMS deve consentire CloudTrail di utilizzare la chiave per crittografare i file di registro e i file digest e consentire agli utenti specificati di leggere i file di registro o i file digest in formato non crittografato. Per informazioni sulla modifica manuale della policy della chiave, consulta Configura le politiche AWS KMS chiave per CloudTrail.

Redazione dell'account proprietario del bucket per gli eventi relativi ai dati richiamati da altri account IDs

Storicamente, se gli eventi CloudTrail relativi ai dati erano abilitati in un chiamante Account AWS dell'API di eventi dati di Amazon S3 CloudTrail , mostrava l'ID account del proprietario del bucket S3 nell'evento dati (ad esempio). `PutObject` Ciò si è verificato anche se l'account proprietario del bucket non ha attivato gli eventi dati S3.

Ora, CloudTrail rimuove l'ID dell'account del proprietario del bucket S3 nel `resources` blocco se vengono soddisfatte entrambe le seguenti condizioni:

- La chiamata API Data Event proviene da un utente Account AWS diverso dal proprietario del bucket Amazon S3.
- Il chiamante API ha ricevuto un errore `AccessDenied` che era solo per l'account chiamante.

Il proprietario della risorsa su cui è stata effettuata la chiamata API riceve ancora l'evento completo.

I seguenti frammenti di record di eventi sono un esempio del comportamento previsto. Nello snippet `Historic`, l'ID account 123456789012 del proprietario del bucket S3 viene mostrato a un chiamante API da un account diverso. Nell'esempio del comportamento corrente, l'ID account del proprietario del bucket non viene visualizzato.

```
# Historic

"resources": [
    {
```

```
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

Di seguito è riportato il comportamento attuale.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

Argomenti

- Impostazione della policy del bucket per più account
- Creazione di percorsi in account aggiuntivi

Impostazione della policy del bucket per più account

Per consentire a un bucket di ricevere file di log da più account, la relativa policy deve concedere a CloudTrail l'autorizzazione per scrivere file di log da tutti gli account specificati. Ciò significa che è necessario modificare la policy del bucket di destinazione per concedere l' CloudTrail autorizzazione a scrivere file di registro da ogni account specificato.

> **Note**
>
> Per motivi di sicurezza, gli utenti non autorizzati non possono creare un percorso che includa `AWSLogs/` come parametro `S3KeyPrefix`.

Per modificare le autorizzazioni del bucket in modo che i file possano essere ricevute da più account

1. Accedi AWS Management Console utilizzando l'account che possiede il bucket (in questo esempio) e apri la console Amazon S3.
2. Scegli il bucket in cui CloudTrail invia i tuoi file di registro, quindi scegli Autorizzazioni.
3. Per Policy del bucket scegli Modifica.
4. Modificare la policy esistente aggiungendo una riga per ogni account aggiuntivo i cui file di log si vuole distribuire a questo bucket. Consulta la seguente policy di esempio e annotare la riga `Resource` sottolineata specificando un secondo ID account. Come best practice per la sicurezza, aggiungi una chiave di condizione `aws:SourceArn` per la policy del bucket Amazon S3. Questo aiuta a prevenire l'accesso non autorizzato al bucket S3. Se hai percorsi esistenti, assicurati di aggiungere una o più chiavi di condizione.

   > **Note**
   >
   > L'ID di un AWS account è un numero di dodici cifre, inclusi gli zeri iniziali.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",

 "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
                    ]
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/111111111111/*",
                "arn:aws:s3:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/222222222222/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",

 "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
                    ],
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Creazione di percorsi in account aggiuntivi

Puoi utilizzare la console o il AWS CLI per creare percorsi aggiuntivi Account AWS e aggregare i relativi file di log in un unico bucket Amazon S3. In alternativa, puoi creare un percorso organizzativo

per registrare tutti gli elementi Account AWS che fanno parte di un'organizzazione. AWS Organizations Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione.

Utilizzo della console per creare percorsi in AWS account aggiuntivi

È possibile utilizzare la CloudTrail console per creare percorsi in account aggiuntivi.

1. Accedi AWS Management Console con l'account per il quale desideri creare un percorso. Completa le operazioni riportate in Creazione di un percorso con la console per creare un percorso usando la console.
2. Per Storage location (Posizione di archiviazione), scegli Use existing S3 bucket (Utilizza bucket S3 esistente). Utilizza la casella di testo per immettere il nome del bucket utilizzato per archiviare i file di log tra gli account.

   > **Note**
   >
   > La bucket policy deve concedere CloudTrail il permesso di scrivervi. Per informazioni sulla modifica manuale della policy bucket, consulta Impostazione della policy del bucket per più account.

3. Per Prefisso, inserisci il prefisso che stai utilizzando per archiviare i file di log tra gli account. Se scegli di utilizzare un prefisso diverso da quello specificato nella policy del bucket, devi modificare la policy del bucket sul bucket di destinazione per consentire CloudTrail la scrittura di file di registro nel bucket utilizzando questo nuovo prefisso.

Utilizzo della CLI per creare un percorso in account aggiuntivi AWS

Puoi utilizzare gli strumenti da riga di AWS comando per creare percorsi in account aggiuntivi e aggregare i relativi file di log in un bucket Amazon S3. Per ulteriori informazioni su questi strumenti, consulta cloudtrail nel Command Reference.AWS CLI

Crea un percorso utilizzando il comando create-trail, specificando quanto segue:

- `--name` specifica il nome del trail.
- `--s3-bucket-name` specifica il bucket Amazon S3 utilizzato per archiviare i file di log tra gli account.

- `--s3-prefix` specifica un prefisso per il percorso di distribuzione dei file di log (opzionale).
- `--is-multi-region-trail`specifica che questo trail registrerà gli eventi in tutte le AWS regioni della partizione in cui stai lavorando.

È possibile creare un percorso per ogni regione in cui un account utilizza risorse. AWS

L'esempio seguente mostra come creare un trail per account aggiuntivi utilizzando la AWS CLI. Per far sì che i file di log per questi account vengano distribuiti nel bucket creato nel primo account (111111111111, in questo esempio), specifica il nome del bucket nell'opzione `--s3-bucket-name`. I nomi dei bucket Amazon S3 devono essere univoci a livello globale.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
multi-region-trail
```

Quando esegui il comando, vedrai un output simile al seguente:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Per ulteriori informazioni sull'utilizzo degli strumenti CloudTrail da riga di AWS comando, consulta il riferimento alla riga di CloudTrail comando.

Condivisione di file di CloudTrail registro tra AWS account

Questa sezione spiega come condividere i file di CloudTrail registro tra più AWS account. L'approccio utilizzato per condividere i log Account AWS dipende dalla configurazione del bucket S3. Di seguito sono riportate le opzioni di condivisione dei file di log:

- Bucket owner applicato: S3 Object Ownership è un'impostazione a livello di bucket Amazon S3 che puoi usare per controllare la proprietà degli oggetti caricati nel tuo bucket e per disabilitare o abilitare le liste di controllo degli accessi (). ACLs Per impostazione predefinita, Object Ownership è impostata sull'impostazione Bucket owner enforced e tutte sono disabilitate. ACLs Quando ACLs

sono disabilitati, il proprietario del bucket possiede tutti gli oggetti nel bucket e gestisce l'accesso ai dati esclusivamente utilizzando le politiche di gestione degli accessi. Quando l'opzione Proprietario del bucket applicato è impostata, l'accesso viene gestito tramite la policy del bucket, eliminando così la necessità per gli utenti di assumere un ruolo.

- Assunzione di un ruolo per condividere i file di log: se non hai scelto l'impostazione Proprietario del bucket applicato, gli utenti dovranno assumere un ruolo per accedere ai file di log nel tuo bucket S3.

Condivisione di file di log tra account tramite l'assunzione di un ruolo

> **Note**
>
> Questa sezione si applica solo ai bucket Amazon S3 che non utilizzano l'impostazione Proprietario del bucket applicato.

Questa sezione spiega come condividere i file di CloudTrail registro tra più persone Account AWS assumendo un ruolo e descrive gli scenari per la condivisione dei file di registro.

- Scenario 1: concedi accesso in sola lettura agli account che hanno generato i file di log inseriti nel bucket Amazon S3.
- Scenario 2: concedi l'accesso a tutti i file di log nel tuo bucket Amazon S3 a un account di terze parti in grado di analizzare i file di log per te.

Per concedere l'accesso in sola lettura ai file di log nel bucket Amazon S3

1. Crea un ruolo IAM per ogni account con cui desideri condividere i file di log. Devi essere un amministratore per poter concedere l'autorizzazione.

   Quando crei il ruolo, procedi nel seguente modo:

   - Scegli l'opzione Un altro Account AWS.
   - Inserisci l'ID a dodici cifre dell'account a cui concedere l'accesso.
   - Selezionare la casella Require MFA (Richiedi MFA) se vuoi che gli utenti forniscano l'autenticazione a più fattori prima di assumere il ruolo.
   - Scegli la politica di AmazonS3 ReadOnlyAccess.

> **Note**
>
> Per impostazione predefinita, la ReadOnlyAccess politica di AmazonS3 concede i diritti di recupero e di elenco per tutti i bucket Amazon S3 all'interno del tuo account.

Per ulteriori dettagli sulla gestione delle autorizzazioni per i ruoli IAM, consulta Ruoli IAM nella Guida per l'utente IAM.

2. Crea una policy di accesso che conceda l'accesso in sola lettura all'account con cui vuoi condividere i file di log.
3. Chiedi a ciascun account di assumere un ruolo per recuperare i file di log.

Per concedere l'accesso in sola lettura ai file di log con account di terze parti

1. Crea un ruolo IAM per l'account di terze parti con cui desideri condividere i file di log. Devi essere un amministratore per poter concedere l'autorizzazione.

   Quando crei il ruolo, procedi nel seguente modo:

   - Scegli l'opzione Un altro Account AWS.
   - Inserisci l'ID a dodici cifre dell'account a cui concedere l'accesso.
   - Inserire un ID esterno che fornisca ulteriore controllo sugli utenti che possono assumere quel ruolo. Per ulteriori informazioni, consulta Come utilizzare un ID esterno per concedere l'accesso alle tue AWS risorse a terzi nella Guida per l'utente IAM.
   - Scegli la politica di AmazonS3 ReadOnlyAccess.

   > **Note**
   >
   > Per impostazione predefinita, la ReadOnlyAccess politica di AmazonS3 concede i diritti di recupero e di elenco per tutti i bucket Amazon S3 all'interno del tuo account.

2. Crea una policy di accesso che conceda l'accesso in sola lettura all'account di terze parti con cui vuoi condividere i file di log.
3. Chiedi all'account di terze parti di assumere un ruolo per recuperare i file di log.

Le seguenti sezioni forniscono maggiori dettagli su questi passaggi.

Argomenti

- Creazione di una policy di accesso per concedere l'accesso ad account di proprietà
- Creazione di una policy di accesso per concedere l'accesso a una terza parte
- Assunzione di un ruolo
- Interrompi la condivisione dei file di CloudTrail registro tra account AWS

Creazione di una policy di accesso per concedere l'accesso ad account di proprietà

In qualità di proprietario del bucket Amazon S3, hai il pieno controllo sul bucket Amazon S3 su cui CloudTrail scrive i file di log per gli altri account. Potresti voler condividere i file di log di ogni unità aziendale con l'unità aziendale che li ha creati. Tuttavia, non vuoi che una business unit sia in grado di leggere i file di log di tutte le altre.

Ad esempio, per condividere i file di log dell'account B con l'account B ma non con l'account C, nell'account A devi creare un nuovo ruolo IAM che specifichi che l'account B è un account attendibile. Questa policy di attendibilità del ruolo specifica che l'account B può essere considerato attendibile per l'assunzione del ruolo creato dall'account A. La policy dovrebbe essere simile all'esempio seguente. La policy di attendibilità viene creata automaticamente se crei il ruolo utilizzando la console. Se utilizzi l'SDK per creare il ruolo, devi specificare la policy di attendibilità come parametro nell'API `CreateRole`. Se utilizzi la CLI per creare il ruolo, devi specificare la policy di attendibilità nel comando CLI `create-role`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
```

```
}
```

Devi inoltre creare una policy di accesso per specificare che l'account B può leggere solo dalla posizione in cui l'account B scrive i propri file di log. La policy di accesso sarà simile all'esempio seguente. Tieni presente che l'ARN della risorsa include l'ID account a dodici cifre per l'account B e l'eventuale prefisso che hai specificato quando hai attivato l'account B durante il processo CloudTrail di aggregazione. Per ulteriori informazioni sulla specifica di un prefisso, consulta Creazione di percorsi in account aggiuntivi.

> **Important**
>
> È necessario assicurarsi che il prefisso nella politica di accesso sia esattamente lo stesso prefisso specificato all'attivazione dell'account B. In caso contrario, è necessario modificare la politica di accesso al ruolo IAM nel proprio account CloudTrail per incorporare il prefisso effettivo per l'account B. Se il prefisso nella politica di accesso al ruolo non è esattamente lo stesso del prefisso specificato all'attivazione dell'account B, l'account B non sarà CloudTrail in grado di accedere ai relativi file di registro.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/account-B-id/
*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
```

```
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

Utilizza il processo precedente anche per gli eventuali account aggiuntivi.

Dopo aver creato i ruoli per ogni account e aver specificato le policy di attendibilità e accesso appropriati, nonché dopo che a un utente IAM in ogni account è stato concesso l'accesso dall'amministratore di tale account, un utente IAM nell'account B o C potrà assumere il ruolo a livello di programmazione.

Per ulteriori informazioni, consulta Assunzione di un ruolo.

Creazione di una policy di accesso per concedere l'accesso a una terza parte

È necessario creare un ruolo IAM separato per un account di terze parti. Quando crei il ruolo, AWS crea automaticamente la relazioni di attendibilità, che specifica che l'account di terze parti è attendibile per l'assunzione del ruolo. La policy di accesso per il ruolo specifica le operazioni che tale account può eseguire. Per ulteriori informazioni sulla creazione dei ruoli, consulta Crea un ruolo IAM.

Ad esempio, la relazione di fiducia creata da AWS specifica che l'account di terze parti (l'account Z in questo esempio) è considerato affidabile per assumere il ruolo che hai creato. Di seguito è illustrato un esempio di policy di attendibilità:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
```

Se quando hai creato il ruolo per l'account di terze parti hai specificato un ID esterno, la policy di accesso contiene un altro elemento `Condition` che verifica l'ID univoco assegnato da tale account. La verifica viene eseguita quando si assume il ruolo. La policy di accesso di esempio seguente contiene un elemento `Condition`.

Per ulteriori informazioni, consulta Come utilizzare un ID esterno per concedere l'accesso alle tue AWS risorse a una terza parte nella Guida per l'utente IAM.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111111111111:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-
account-Z"}}
    }]
}
```

Devi inoltre creare una policy di accesso per il tuo account per specificare che l'account di terze parti può leggere tutti i log nel bucket Amazon S3. La policy di accesso dovrebbe essere simile all'esempio seguente. Il carattere jolly (*) dopo il valore `Resource` indica che l'account di terze parti può accedere a qualsiasi file di log nel bucket S3 per il quale dispone dell'accesso.

JSON

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

```
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

Dopo aver creato un ruolo per l'account di terze parti e aver specificato la relazione di attendibilità e la policy di accesso corrette, un utente IAM nell'account di terze parti deve assumere il ruolo a livello di programmazione in modo da poter leggere i file di log nel bucket. Per ulteriori informazioni, consulta Assunzione di un ruolo.

Assunzione di un ruolo

Devi designare un utente IAM separato per assumere ogni ruolo che crei in ogni account. Devi quindi assicurarti che ogni utente IAM disponga delle autorizzazioni appropriate.

Utenti e ruoli IAM

Dopo aver creato i ruoli e le policy necessari, devi definire un utente IAM in ciascuno degli account con cui desideri condividere i file. Ogni utente IAM assume il ruolo corretto a livello di programmazione per accedere ai file di log. Quando un utente assume un ruolo, AWS restituisce credenziali di sicurezza temporanee a tale utente. Possono quindi effettuare richieste per elencare, recuperare, copiare o eliminare i file di log a seconda delle autorizzazioni concesse dalla policy di accesso associata al ruolo.

Per ulteriori informazioni sulle diverse identità IAM, consulta Identità IAM (utenti, gruppi di utenti e ruoli).

La differenza principale risiede nella policy di accesso creata per ogni ruolo IAM in ogni scenario.

- Nello scenario 1, la policy di accesso limita ogni account alle operazioni di lettura solo dei propri file di log. Per ulteriori informazioni, consulta Creazione di una policy di accesso per concedere l'accesso ad account di proprietà.
- Nello scenario 2, la policy di accesso permette a un account di terze parti di leggere tutti i file di log aggregati nel bucket Amazon S3. Per ulteriori informazioni, consulta Creazione di una policy di accesso per concedere l'accesso a una terza parte.

Creazione delle policy di autorizzazione per gli utenti IAM

Per eseguire le azioni consentite da un ruolo, l'utente IAM deve avere il permesso di chiamare l' AWS STS `AssumeRole`API. Devi modificare la policy per ogni utente in modo da concedere le autorizzazioni appropriate. In altre parole, devi impostare un elemento Risorsa nella policy collegata all'utente IAM. L'esempio seguente mostra una policy per un utente IAM in un altro account che permette a tale utente di assumere un ruolo denominato `Test` creato in precedenza dall'account A.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/Test"
        }
    ]
}
```

Per modificare una policy gestita dal cliente (console)

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Policy.
3. Nell'elenco delle policy, selezionare il nome della policy da modificare. Puoi utilizzare la casella di ricerca per filtrare l'elenco di policy.

4. Seleziona la scheda Autorizzazioni e scegli Modifica.
5. Esegui una di queste operazioni:
   - Per modificare la policy senza conoscere la sintassi JSON, seleziona l'opzione Visivo. Puoi modificare servizi, operazioni, risorse o condizioni opzionali per ogni blocco di autorizzazione della policy. Inoltre, puoi importare una policy per aggiungere ulteriori autorizzazioni nella parte finale. Al termine, seleziona Successivo per continuare.
   - Seleziona la scheda JSON per modificare la policy, digitando o copiando il testo nella casella JSON. Inoltre, puoi importare una policy per aggiungere ulteriori autorizzazioni nella parte finale. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la convalida delle policy, quindi scegli Next (Successivo).

     > **Note**
     >
     > È possibile alternare le opzioni dell'editor Visivo e JSON in qualsiasi momento. Se tuttavia si apportano modifiche o si seleziona Successivo nell'editor Visivo, IAM potrebbe ristrutturare la policy in modo da ottimizzarla per l'editor visivo. Per ulteriori informazioni, consulta Modifica della struttura delle policy nella Guida per l'utente di IAM.
6. Nella pagina Verifica e salva, esamina il campo Autorizzazioni definite in questa policy, quindi scegli Salva modifiche per salvare il lavoro.
7. Se esistono già un massimo di cinque versioni della policy gestita, seleziona Salva per visualizzare una finestra di dialogo. Per salvare la nuova versione, la versione non predefinita più vecchia della policy viene rimossa e sostituita con la nuova. Facoltativamente, puoi impostare la nuova versione come versione predefinita della policy.

   Scegli Salva modifiche per salvare la nuova versione della policy.

Chiamata AssumeRole

Un utente può assumere un ruolo creando un'applicazione che richiama l' AWS STS `AssumeRole`API e trasmette il nome della sessione del ruolo, l'Amazon Resource Number (ARN) del ruolo da assumere e un ID esterno opzionale. Il nome della sessione del ruolo viene definito dall'account che ha creato il ruolo da assumere. L'eventuale ID esterno viene definito dall'account di terze parti e passato all'account proprietario per essere incluso durante la creazione del ruolo. Per ulteriori informazioni, consulta Come utilizzare un ID esterno per concedere l'accesso alle tue AWS

risorse a terzi nella Guida per l'utente IAM. Puoi recuperare l'ARN dall'account A aprendo la console IAM.

Per individuare il valore ARN nell'account A con la console IAM

1. Selezionare Roles (Ruoli).
2. Scegliere il ruolo da esaminare.
3. Cercare il valore in Role ARN (ARN ruolo) nella sezione Summary (Riepilogo).

L' AssumeRole API restituisce credenziali temporanee da utilizzare per accedere alle risorse dell'account proprietario. In questo esempio, le risorse a cui desideri accedere sono il bucket Amazon S3 e i file di log al suo interno. Le credenziali temporanee dispongono delle autorizzazioni definite nella policy di accesso del ruolo.

Il seguente esempio Python (che utilizza AWS SDK for Python (Boto)) mostra come chiamare `AssumeRole` e come utilizzare le credenziali di sicurezza temporanee restituite per elencare tutti i bucket Amazon S3 controllati dall'account A.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
```

```
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

Interrompi la condivisione dei file di CloudTrail registro tra account AWS

Per interrompere la condivisione dei file di registro con un altro Account AWS, elimina il ruolo che hai creato per quell'account. Per informazioni sull'eliminazione di un ruolo, consulta Eliminazione di ruoli o profili delle istanze.

Convalida dell'integrità dei file di CloudTrail registro

Per determinare se un file di registro è stato modificato, eliminato o immutato dopo la CloudTrail consegna, è possibile utilizzare la convalida dell'integrità del file di CloudTrail registro. Questa caratteristica è stata sviluppata utilizzando algoritmi standard di settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail È possibile utilizzare il AWS CLI per convalidare i file nella posizione in cui sono stati consegnati. CloudTrail

Perché usare questa funzionalità?

I file di log convalidati sono preziosi nelle indagini giudiziarie e sulla sicurezza. Ad esempio, un file di log convalidato consente di confermare senza ombra di dubbio che tale file non ha subito modifiche oppure che una specifica attività API è stata eseguita utilizzando credenziali utente attendibili. Il processo di convalida dell'integrità dei file di CloudTrail registro consente inoltre di sapere se un file di registro è stato eliminato o modificato o di affermare con certezza che nessun file di registro è stato inviato all'account durante un determinato periodo di tempo.

Come funziona

Quando abiliti la convalida dell'integrità dei file di registro, CloudTrail crea un hash per ogni file di registro fornito. Ogni ora, CloudTrail inoltre, crea e consegna un file che fa riferimento ai file di registro dell'ultima ora e contiene un hash di ciascuno di essi. Questo file è chiamato file digest. CloudTrail firma ogni file digest utilizzando la chiave privata di una coppia di chiavi pubblica e privata. Dopo la consegna, è possibile utilizzare la chiave pubblica per convalidare il file digest. CloudTrail utilizza coppie di chiavi diverse per ciascuna. Regione AWS

I file digest vengono inviati allo stesso bucket Amazon S3 associato al percorso dei file di log. CloudTrail Se i tuoi file di log vengono distribuiti da tutte le regioni o da più account in un unico bucket Amazon S3, CloudTrail distribuirà i file digest di tali regioni e account nello stesso bucket.

I file digest vengono inseriti in una cartella distinta rispetto a quella dei file di log. Questa separazione tra file digest e file di log ti consente di applicare policy di sicurezza granulare e di garantire il corretto funzionamento senza modifiche delle soluzioni di elaborazione dei log esistenti. Ogni file digest contiene anche la firma digitale dei file di digest precedente, se esistente. La firma del file digest corrente è memorizzata nelle proprietà metadati dell'oggetto file digest Amazon S3. Per ulteriori informazioni sul contenuto dei file digest, consulta CloudTrail struttura del file digest.

Storage dei file di log e file digest

Puoi archiviare i file di CloudTrail log e i file digest in Amazon S3 o S3 Glacier in modo sicuro, duraturo ed economico per un periodo di tempo indefinito. Per ottimizzare la sicurezza dei file digest archiviati in Amazon S3, puoi utilizzare la funzionalità di eliminazione MFA di Amazon S3.

Abilitazione della convalida e convalida dei file

Per abilitare la convalida dell'integrità dei file di log, puoi utilizzare l'API, the o. AWS Management Console AWS CLI CloudTrail L'abilitazione della convalida dell'integrità dei file di log consente

di CloudTrail inviare file di log digest al bucket Amazon S3, ma non convalida l'integrità dei file. Per ulteriori informazioni, consulta Abilitazione della convalida dell'integrità dei file di registro per CloudTrail.

Per convalidare l'integrità dei file di CloudTrail log, puoi utilizzare o creare una soluzione personalizzata. AWS CLI AWS CLI Convaliderà i file nella posizione in cui sono CloudTrail stati consegnati. Se desideri convalidare i log che sono stati spostati in un percorso diverso, in Amazon S3 o in un'altra posizione, puoi creare strumenti di convalida personalizzati.

Per informazioni sulla convalida dei log utilizzando il AWS CLI, vedere. Convalida dell'integrità dei file di CloudTrail registro con AWS CLI Per informazioni sullo sviluppo di implementazioni personalizzate per la convalida dei file di CloudTrail registro, vedere. Implementazioni personalizzate della convalida dell'integrità dei file di CloudTrail registro

Abilitazione della convalida dell'integrità dei file di registro per CloudTrail

È possibile abilitare la convalida dell'integrità dei file di registro utilizzando l' AWS Management Console interfaccia a riga di AWS comando (AWS CLI) o l' CloudTrail API. CloudTrail inizia a consegnare i file digest in circa un'ora.

AWS Management Console

Per abilitare la convalida dell'integrità dei file di registro con la CloudTrail console, scegli Sì per l'opzione Abilita la convalida dei file di registro quando crei o aggiorni un trail. Per impostazione di default, questa caratteristica è abilitata per nuovi trail. Per ulteriori informazioni, consulta Creazione e aggiornamento di un percorso con la console.

AWS CLI

Per abilitare la convalida dell'integrità dei file di registro con AWS CLI, utilizza l'`--enable-log-file-validation`opzione con i comandi create-trail o update-trail. Per disabilitare la convalida dell'integrità dei file di log per un trail, usa l'opzione `--no-enable-log-file-validation`.

Esempio

Il seguente comando `update-trail` abilita la convalida dei file di log e avvia la distribuzione dei file digest al bucket Amazon S3 per il percorso specificato.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

Per abilitare la convalida dell'integrità dei file di registro con l' CloudTrail API, imposta il parametro di `EnableLogFileValidation` richiesta su `true` quando chiami `CreateTrail` o`UpdateTrail`.

Per ulteriori informazioni, consulta le pagine CreateTrail e UpdateTrail nella Documentazione di riferimento dell'API AWS CloudTrail.

Convalida dell'integrità dei file di CloudTrail registro con AWS CLI

Per convalidare i log con AWS Command Line Interface, utilizzare il CloudTrail `validate-logs` comando. Il comando utilizza i file digest distribuiti nel bucket Amazon S3 per eseguire la convalida. Per informazioni sui file digest, consulta CloudTrail struttura del file digest.

AWS CLI Consente di rilevare i seguenti tipi di modifiche:

- Modifica o cancellazione dei file di CloudTrail registro
- Modifica o eliminazione dei file CloudTrail digest
- Modifica o eliminazione di entrambi i tipi di file

> **Note**
>
> AWS CLI Convalida solo i file di registro a cui fanno riferimento i file digest. Per ulteriori informazioni, consulta Verifica se un determinato file è stato consegnato da CloudTrail.

Prerequisiti

Per convalidare l'integrità dei file di registro con AWS CLI, devono essere soddisfatte le seguenti condizioni:

- È necessario disporre di una connettività online a. AWS
- Devi disporre dell'accesso in lettura al bucket Amazon S3 contenente i file digest e i file di log.
- Il digest e i file di log non devono essere stati spostati dalla posizione originale di Amazon S3 CloudTrail in cui sono stati consegnati.
- Il ruolo che esegue il comando deve disporre delle autorizzazioni per la chiamata `ListObjects` e `GetBucketLocation` per ogni bucket S3 a cui fa riferimento il trail. `GetObject`

> **Note**
>
> I file di log scaricati su un disco locale non possono essere convalidati mediante la AWS CLI. Per istruzioni su come creare strumenti personalizzati per la convalida, consulta Implementazioni personalizzate della convalida dell'integrità dei file di CloudTrail registro.

validate-logs

Sintassi

Di seguito è riportata la sintassi per `validate-logs`. I parametri opzionali sono riportati tra parentesi.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <amzn-s3-demo-bucket>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> Il comando `validate-logs` è specifico della Regione. È necessario specificare l'opzione `--region` globale per convalidare i log per uno specifico. Regione AWS

Opzioni

Di seguito sono elencati le opzioni dalla riga di comando per `validate-logs`. Le opzioni `--trail-arn` e `--start-time` sono obbligatorie. L'opzione `--account-id` è inoltre necessaria per i percorsi organizzativi.

`--start-time`

Specifica che i file di log vengano distribuiti in corrispondenza della o dopo la convalida il valore del time stamp UTC specificato. Esempio: `2015-01-08T05:21:42Z`.

`--end-time`

(Opzionale) Specifica che i file di log vengano distribuiti in corrispondenza o prima della convalida il valore del time stamp UTC specificato. Il valore di default è l'ora UTC corrente (`Date.now()`). Esempio: `2015-01-08T12:31:41Z`.

> **Note**
>
> Per l'intervallo di tempo specificato, il comando `validate-logs` controlla solo i file di log per i quali esistono riferimenti nei corrispondenti file digest. Non viene controllato alcun altro file di log nel bucket Amazon S3. Per ulteriori informazioni, consulta Verifica se un determinato file è stato consegnato da CloudTrail.

`--s3-bucket`

Facoltativamente, specifica il bucket Amazon S3 in cui vengono archiviati i file digest. Se non viene specificato il nome di un bucket, lo AWS CLI recupererà chiamando. `DescribeTrails()`

`--s3-prefix`

Facoltativamente, specifica il prefisso Amazon S3 in cui vengono archiviati i file digest. Se non viene specificato, lo AWS CLI recupererà chiamando. `DescribeTrails()`

> **Note**
>
> È consigliabile utilizzare questa opzione solo se il prefisso corrente è diverso dal prefisso in uso durante l'intervallo di tempo specificato.

`--account-id`

Facoltativamente, specifica l'account per la convalida dei log. Questo parametro è necessario per i percorsi organizzativi per la convalida dei log per l'account specifico all'interno di un'organizzazione.

`--trail-arn`

Specifica l'ARN (Amazon Resource Name) del trail da convalidare. Il formato dell'ARN di un trail è riportato di seguito.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Per recuperare l'ARN per un trail, puoi utilizzare il comando `describe-trails` prima di eseguire `validate-logs`.
> Potresti decidere di specificare il nome e il prefisso del bucket, oltre al relativo ARN, se i file di log sono stati distribuiti in più di un bucket nell'intervallo di tempo specificato e vuoi limitare il processo di convalida ai file di log in uno solo dei bucket.

`--verbose`

(Opzionale) Restituisce le informazioni di convalida per ogni file di log o file digest nell'intervallo di tempo specificato. L'output indica se il file è rimasto invariato o se è stato modificato o eliminato. In modalità non dettagliata (impostazione di default), le informazioni vengono restituite solo nei casi in cui si è verificato un errore di convalida.

Esempio

L'esempio seguente consente di convalidare i file di log dall'ora di inizio specificata all'ora corrente utilizzando il bucket Amazon S3 configurato per il percorso corrente e specificando l'output dettagliato.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

Funzionamento di **`validate-logs`**

Il comando `validate-logs` inizia con la convalida del file digest più recente nell'intervallo di tempo specificato. In primo luogo, verifica se il file digest è stato scaricato da un percorso a cui il file effettivamente appartiene. In altre parole, se la CLI ha scaricato il file digest `df1` dal percorso S3 `p1`, validate-logs verificherà quanto segue: `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

Se la firma del file digest è valida, controlla il valore hash di ciascuno dei log a cui viene fatto riferimento nel file digest. Il comando va a ritroso nel tempo e convalida i file digest precedenti e i corrispondenti file di log di riferimento, in sequenza. Continua il processo fino al raggiungimento del valore specificato per `start-time` o fino al termine della sequenza di file digest. Se un file digest

non è disponibile o non è valido, l'intervallo di tempo che non può essere convalidato è indicato nell'output.

Risultati della convalida

I risultati della convalida iniziano con un'intestazione di riepilogo avente il formato seguente:

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

Ogni riga dell'output principale contiene i risultati della convalida per un singolo file digest o file di log nel formato seguente:

```
<Digest file | Log file> <S3 path> <Validation Message>
```

Nella tabella riportata di seguito sono descritti i possibili messaggi di convalida per i file di log e i file digest.

Tipo di file	Messaggio di convalida	Descrizione
`Digest file`	`valid`	La firma del file digest è valida. I file di log a cui fa riferimento possono essere controlla ti. Questo messaggio è incluso solo nella modalità dettagliata (verbose).
`Digest file`	`INVALID: has been moved from its original location`	Il bucket S3 o l'oggetto S3 da cui il file digest è stato recuperato non corrisponde alla posizione del bucket S3 o a quella dell'ogge tto S3 registrate nel file digest stesso.
`Digest file`	`INVALID: invalid format`	Il formato del file digest non è valido. I file di log corrispondenti all'intervallo di tempo rappresentato dal file digest non può essere convalidato.
`Digest file`	`INVALID: not found`	Il file digest non è stato trovato. I file di log corrispondenti all'intervallo di tempo rappresentato dal file digest non può essere convalidato.

Tipo di file	Messaggio di convalida	Descrizione
`Digest file`	`INVALID: public key not found for fingerprint` *`fingerprint`*	La chiave pubblica corrispondente alla impronta registrata nel file digest non è stata trovata. Il file digest non può essere convalidato.
`Digest file`	`INVALID: signature verification failed`	La firma del file digest non è valida. Poiché il file digest non è valido, i file di log a cui fa riferimento non possono essere convalidati e non è possibile effettuare alcuna asserzione sulla corrispondente attività delle API.
`Digest file`	`INVALID: Unable to load PKCS #1 key with fingerprint` *`fingerprint`*	Poiché è risultato impossibile caricare la chiave pubblica con codifica DER nel formato PKCS # 1 e con l'impronta specifica ta, il file digest non può essere convalidato.
`Log file`	`valid`	Il file di log è stato convalidato e non è stato modificato dopo la distribuzione. Questo messaggio è incluso solo nella modalità dettagliata (verbose).
`Log file`	`INVALID: hash value doesn't match`	L'hash per il file di log non corrisponde. Il file di log è stato modificato dopo la distribuz ione da parte di CloudTrail.
`Log file`	`INVALID: invalid format`	Il formato del file di log non è valido. Il file di log non può essere convalidato.
`Log file`	`INVALID: not found`	Il file di log non è stato trovato e non può essere convalidato.

L'output include informazioni riepilogative sui risultati restituiti.

Output di esempio

Modalità dettagliata

Il comando `validate-logs` di esempio seguente utilizza il flag `--verbose` e restituisce l'output di esempio seguente. `[...]` indica che l'output di esempio è stato abbreviato.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
```

```
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://amzn-s3-demo-bucketAWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid
```

```
Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Modalità non dettagliata

Il comando `validate-logs` di esempio seguente non utilizza il flag `--verbose`. Nell'output di esempio che segue è stato rilevato un errore. Vengono restituite solo le informazioni relative a intestazione, errori e riepilogo.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Verifica se un determinato file è stato consegnato da CloudTrail

Per verificare se un particolare file nel tuo bucket è stato consegnato da CloudTrail, eseguilo `validate-logs` in modalità dettagliata per il periodo di tempo che include il file. Se il file appare nell'output di`validate-logs`, allora il file è stato consegnato da. CloudTrail

CloudTrail struttura del file digest

Ogni file digest contiene i nomi dei file di log distribuiti nel bucket Amazon S3 durante l'ultima ora, i valori hash per tali file di log e la firma digitale del file di digest precedente. La firma del file digest corrente è memorizzata nelle proprietà metadati dell'oggetto file digest. Le firme digitali e gli hash vengono utilizzati per la convalida dell'integrità dei file di log e del file digest stesso.

Posizione dei file digest

I file digest vengono distribuiti in un bucket Amazon S3 il cui percorso è conforme alla seguente sintassi.

```
s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> Per i trail dell'organizzazione, la posizione del bucket include anche l'ID dell'unità organizzativa, come segue:
>
> ```
> s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>  region/digest-end-year/digest-end-month/digest-end-date/
>  aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

Contenuto dei file digest di esempio

Il seguente file digest di esempio contiene informazioni per un CloudTrail registro.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "amzn-s3-demo-bucket",
```

```
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "amzn-s3-demo-bucket",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

Descrizione dei campi dei file digest

Di seguito sono riportate descrizioni di ciascun campo del file digest:

`awsAccountId`

L'ID AWS dell'account per il quale è stato consegnato il file digest.

`digestStartTime`

L'intervallo di tempo UTC iniziale coperto dal file digest, prendendo come riferimento l'ora in cui i file di registro sono stati consegnati. CloudTrail Ciò significa che se l'intervallo di tempo è [Ta, Tb], il file digest conterrà tutti i file di log distribuiti al cliente tra Ta e Tb.

`digestEndTime`

L'intervallo di tempo UTC finale coperto dal file digest, prendendo come riferimento l'ora in cui i file di registro sono stati consegnati. CloudTrail Ciò significa che se l'intervallo di tempo è [Ta, Tb], il file digest conterrà tutti i file di log distribuiti al cliente tra Ta e Tb.

`digestS3Bucket`

Nome del bucket Amazon S3 in cui il file digest corrente è stato distribuito.

`digestS3Object`

Chiave dell'oggetto Amazon S3 (ovvero il percorso del bucket Amazon S3) del file digest corrente. Le prime due Regioni nella stringa mostrano la Regione da cui il file digest è stato distribuito. L'ultima Regione (dopo `your-trail-name`) è la Regione di origine del percorso. La Regione di origine è la Regione in cui è stato creato il percorso. Nel caso di un percorso multi-regione, la Regione potrebbe essere diversa da quella da cui il file digest è stato distribuito.

`newestEventTime`

Ora, in formato UTC, dell'evento più recente rispetto a tutti gli eventi nei file di log inclusi nel file digest.

`oldestEventTime`

Ora, in formato UTC, dell'evento meno recente rispetto a tutti gli eventi nei file di log inclusi nel file digest.

> **Note**
>
> Se il file digest viene distribuito in ritardo, il valore di `oldestEventTime` sarà anteriore al valore di `digestStartTime`.

`previousDigestS3Bucket`

Bucket Amazon S3 in cui il precedente file digest è stato distribuito.

`previousDigestS3Object`

Chiave dell'oggetto Amazon S3 (ovvero il percorso del bucket Amazon S3) del file digest precedente.

`previousDigestHashValue`

Valore hash con codifica esadecimale dei contenuti non compressi del file digest precedente.

`previousDigestHashAlgorithm`

Nome dell'algoritmo hash utilizzato per eseguire l'hashing del file digest precedente.

`publicKeyFingerprint`

Impronta con codifica esadecimale della chiave pubblica corrispondente alla chiave privata utilizzata per firmare il file digest. È possibile recuperare le chiavi pubbliche per l'intervallo di tempo corrispondente al file digest utilizzando o l' AWS CLI API. CloudTrail Tra le chiavi pubbliche restituite, la chiave la cui impronta corrisponde a questo valore può essere usata per convalidare il file digest. Per informazioni sul recupero delle chiavi pubbliche per i file digest, consulta il comando o l' AWS CLI `list-public-keys`API. CloudTrail `ListPublicKeys`

> **Note**
>
> CloudTrail utilizza diverse coppie di chiavi pubblice/private per regione. Ogni file digest è firmato con una chiave privata univoca per la Regione corrispondente. Pertanto, quando convalidi un file digest di una determinata Regione, nella stessa Regione devi recuperare la corrispondente chiave pubblica.

`digestSignatureAlgorithm`

Algoritmo usato per firmare il file digest.

`logFiles.s3Bucket`

Nome del bucket Amazon S3 per il file di log.

`logFiles.s3Object`

Chiave dell'oggetto Amazon S3 del file di log corrente.

`logFiles.newestEventTime`

Ora, in formato UTC, dell'evento più recente nel file di log. Questa ora corrisponde inoltre al time stamp del file di log stesso.

`logFiles.oldestEventTime`

Ora, in formato UTC, dell'evento meno recente nel file di log.

`logFiles.hashValue`

Valore hash con codifica esadecimale del contenuto non compresso del file di log.

`logFiles.hashAlgorithm`

Algoritmo hash usato per eseguire l'hashing del file di log.

File digest di iniziale

Quando viene avviata la convalida dell'integrità dei file di log, verrà generato un file digest iniziale. Un file digest iniziale verrà generato anche quando viene riavviata la convalida dell'integrità dei file di log (mediante la disabilitazione e quindi la riabilitazione di tale processo di convalida oppure mediante l'arresto e il riavvio della registrazione con la convalida abilitata). In un file digest iniziale, i seguenti campi relativi al file digest precedente saranno null:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

File digest 'vuoti'

CloudTrail fornirà un file digest anche se non vi è stata alcuna attività API nel tuo account durante il periodo di un'ora rappresentato dal file digest. Ciò può essere utile quando è necessario verificare che non sono stati distribuiti file di log durante l'ora di riferimento del file digest.

L'esempio seguente mostra i contenuti di un file digest contenente un'ora di registrazione in assenza di qualsiasi tipo di attività API. Si noti che il campo `logFiles:[ ]` alla fine del contenuto del file digest è vuoto.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "amzn-s3-demo-bucket",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

Firma del file digest

Le informazioni sulla firma di un file digest si trovano in due proprietà metadati dell'oggetto file digest Amazon S3. Ogni file digest include le seguenti voci di metadati:

- `x-amz-meta-signature`

  Valore con codifica esadecimale della firma del file digest. Di seguito è riportata una firma di esempio:

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e7100905176946923 1bc22232fa260df02740047af532229
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  L'esempio seguente mostra un valore dell'algoritmo utilizzato per generare la firma del file digest:

  `SHA256withRSA`

Concatenamento di file digest

Il fatto che ogni file digest contenga un riferimento al file digest precedente consente un «concatenamento» che consente a strumenti di convalida come il di AWS CLI rilevare se un file digest è stato eliminato. Consente inoltre ai file digest di un intervallo di tempo specificato di venire controllati in successione, a partire dal file più recente.

> **Note**
>
> Quando si disabilita la convalida dell'integrità dei file di registro, la catena di file digest viene interrotta dopo un'ora. CloudTrail non creerà file digest per i file di registro che sono stati consegnati durante un periodo in cui la convalida dell'integrità dei file di registro era disabilitata. Ad esempio, se si abilita la convalida dell'integrità dei file di log a mezzogiorno del 1° gennaio, la si disabilita a mezzogiorno del 2 gennaio e la si abilita di nuovo a mezzogiorno del 10 gennaio, non verranno creati file digest per i file di log distribuiti da mezzogiorno del 2 gennaio a mezzogiorno del 10 gennaio. Lo stesso vale ogni volta che si interrompe CloudTrail la registrazione o si elimina una traccia.

Se la policy del bucket S3 del tuo trail non è configurata correttamente o si verifica CloudTrail un'interruzione imprevista del servizio, potresti non ricevere tutti o alcuni file digest. Per confermare se il trail presenta errori di consegna del digest, esegui il `get-trail-status`comando e verifica la presenza di errori nel parametro. `LatestDigestDeliveryError` Dopo aver risolto il problema di consegna (ad esempio, correggendo la policy del bucket), CloudTrail tenterà di recapitare i file digest mancanti. Durante il periodo di riconsegna, i file digest potrebbero essere consegnati fuori servizio, pertanto la catena potrebbe sembrare temporaneamente interrotta.

Se la registrazione viene interrotta o la traccia viene eliminata, CloudTrail consegnerà un file digest finale. Questo file digest può contenere informazioni per qualsiasi file di log rimanente che fa riferimento fino all'evento `StopLogging` compreso.

Implementazioni personalizzate della convalida dell'integrità dei file di CloudTrail registro

Poiché CloudTrail utilizza algoritmi crittografici e funzioni hash standard del settore e disponibili apertamente, è possibile creare strumenti personalizzati per convalidare l'integrità dei file di registro. CloudTrail Quando la convalida dell'integrità dei file di log è abilitata, CloudTrail invia i file digest al tuo bucket Amazon S3. Puoi utilizzare questi file per implementare la tua soluzione di convalida personalizzata. Per ulteriori informazioni sui file digest, consulta CloudTrail struttura del file digest.

Questo argomento descrive come vengono firmati i file digest e illustra in dettaglio le procedure necessarie per implementare una soluzione che convalida i file digest e i file di log a cui fanno riferimento.

Comprendere come CloudTrail vengono firmati i file digest

CloudTrail i file digest sono firmati con firme digitali RSA. Per ogni file digest, CloudTrail esegue le seguenti operazioni:

1. Crea una stringa per la firma dei dati in base ai campi del file digest designato (descritti nella sezione successiva).
2. Recupera una chiave privata univoca per la Regione.
3. Passa l'hash SHA-256 della stringa e la chiave privata all'algoritmo di firma RSA, che genera una firma digitale.
4. Codifica il codice byte della firma in formato esadecimale.
5. Inserisce la firma digitale nella proprietà metadati `x-amz-meta-signature` dell'oggetto file digest Amazon S3.

Contenuto della stringa di firma dei dati

I seguenti CloudTrail oggetti sono inclusi nella stringa per la firma dei dati:

- Time stamp finale del file digest nel formato UTC esteso (ad esempio, `2015-05-08T07:19:37Z`)
- Percorso S3 del file digest corrente
- Hash SHA-256 con codifica esadecimale del file digest corrente
- Firma con codifica esadecimale del precedente file digest

Il formato per calcolare questa stringa e un esempio di stringa vengono forniti più avanti in questo documento.

Fasi di implementazione della convalida personalizzata

Durante l'implementazione di una soluzione di convalida personalizzata, devi convalidare il file digest per primo e quindi i file di log a cui fa riferimento.

Convalida del file digest

Per convalidare un file digest, devi disporre della relativa firma, della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file e di una stringa di firma dei dati che elaborerai personalmente.

1. Recuperare il file digest.
2. Verificare che il file digest sia stato recuperato dal relativo percorso originale.
3. Recuperare la firma con codifica esadecimale del file digest.
4. Recuperare l'impronta con codifica esadecimale della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file digest.
5. Recuperate le chiavi pubbliche per l'intervallo di tempo corrispondente al file digest.
6. Tra le chiavi pubbliche recuperate scegliere la chiave pubblica con l'impronta corrispondente a quella nel file digest.
7. Utilizzando l'hash del file digest e gli altri campi del file, ricreare la stringa di firma dei dati per verificare la firma del file digest.
8. Per convalidare la firma, passare l'hash SHA-256 della stringa, la chiave pubblica e la firma come parametri all'algoritmo RSA di verifica della firma. Se il risultato è true, il file digest è valido.

Convalida dei file di log

Se il file digest è valido, convalidare ciascun file di log a cui il file digest fa riferimento.

1. Per convalidare l'integrità di un file di log, calcolare il relativo valore hash SHA-256 per il relativo contenuto non compresso e confrontare i risultati con il valore hash per il file di log registrato in formato esadecimale nel digest. Se i valori hash corrispondono, il file di log è valido.
2. Utilizzando le informazioni relative al file digest precedente incluse nel file digest corrente, convalidare in sequenza i file digest precedenti e i corrispondenti file di log.

Le seguenti sezioni descrivono in dettaglio queste fasi.

A. Recupero del file digest

Durante la fase iniziale di recupero del file digest più recente, devi assicurarsi di avere recuperato il file dalla relativa posizione originale, verificarne la firma digitale e recuperare l'impronta della chiave pubblica.

1. Utilizzando S3 `GetObject`o la classe AmazonS3Client (ad esempio), ottieni il file digest più recente dal tuo bucket Amazon S3 per l'intervallo di tempo che desideri convalidare.
2. Verificare che il bucket S3 e l'oggetto S3 utilizzati per recuperare il file corrispondano alla posizione del bucket S3 e a quella dell'oggetto S3 registrate nel file digest stesso.
3. Recupera quindi la firma digitale del file digest dalla proprietà metadati `x-amz-meta-signature` dell'oggetto del file digest in Amazon S3.
4. Nel file digest recuperare l'impronta della chiave pubblica la cui chiave privata è stata utilizzata per firmare il file digest dal campo `digestPublicKeyFingerprint`.

B. Recupero della chiave pubblica per la convalida del file digest

Per ottenere la chiave pubblica per convalidare il file digest, puoi utilizzare l'o l'API. AWS CLI CloudTrail In entrambi i casi, puoi specificare un intervallo di tempo (ovvero un'ora di inizio e una di fine) per il file digest da convalidare. È possibile che vengano restituite una o più chiavi pubbliche per l'intervallo di tempo specificato. Le chiavi restituite possono avere intervalli di tempo di validità sovrapposti.

> **Note**
>
> Poiché CloudTrail utilizza diverse coppie di chiavi pubblice/private per regione, ogni file digest è firmato con una chiave privata unica per la sua regione. Pertanto, quando convalidi un file digest da una determinata Regione, devi recuperare la relativa chiave pubblica dalla stessa Regione.

Usa il per recuperare le chiavi pubbliche AWS CLI

Per recuperare le chiavi pubbliche per i file digest utilizzando il AWS CLI, usa il comando. `cloudtrail list-public-keys` Il comando ha il formato seguente:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time
<end-time>]
```

I parametri relativi all'ora di inizio e all'ora di fine sono time stamp UTC facoltativi. Se non specificata, verrà utilizzata l'ora corrente e verranno restituite la chiave o le chiavi pubbliche attualmente attive.

Risposta di esempio

La risposta sarà un elenco di oggetti JSON che rappresentano la chiave o le chiavi restituite:


```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
```

```
    ]
}
```

Utilizza l' CloudTrail API per recuperare le chiavi pubbliche

Per recuperare le chiavi pubbliche per i file digest utilizzando l' CloudTrail API, trasmetti i valori dell'ora di inizio e dell'ora di fine all'API. `ListPublicKeys` L'API `ListPublicKeys` restituisce le chiavi pubbliche le cui chiavi private sono state utilizzate per firmare i file digest compresi nell'intervallo di tempo specificato. Per ogni chiave pubblica, l'API restituisce anche le corrispondenti impronte.

`ListPublicKeys`

Questa sezione descrive i parametri di richiesta e gli elementi di risposta dell'API `ListPublicKeys`.

> **Note**
>
> La codifica dei campi binari per `ListPublicKeys` è soggetta a modifiche.

Parametri della richiesta

Nome	Descrizione
`StartTime`	Facoltativamente, in UTC, l'inizio dell'intervallo di tempo per la ricerca delle chiavi pubbliche per i file digest. CloudTrail Se non StartTime è specificato, viene utilizzata l'ora corrente e viene restituita la chiave pubblica corrente. Tipo: DateTime
`EndTime`	Facoltativamente, specifica, in UTC, la fine dell'intervallo di tempo in cui cercare le chiavi pubbliche per CloudTrail i file digest. Se non EndTime è specificato, viene utilizzata l'ora corrente. Tipo: DateTime

Elementi di risposta

`PublicKeyList`, una matrice di oggetti `PublicKey` contenenti:

Nome	Descrizione
`Value`	Valore della chiave pubblica con codifica DER in formato PKCS #1. Tipo: Blob
`ValidityStartTime`	Ora di inizio della validità della chiave pubblica. Tipo: DateTime
`ValidityEndTime`	Ora di fine della validità della chiave pubblica. Tipo: DateTime
`Fingerprint`	Impronta della chiave pubblica. L'impronta può essere utilizzata per identificare la chiave pubblica da utilizzare per convalidare il file digest. Tipo: stringa

C. Scelta della chiave pubblica da utilizzare per la convalida

Tra le chiavi pubbliche recuperate da `list-public-keys` o `ListPublicKeys`scegliere la chiave pubblica restituita con l'impronta corrispondente all'impronta registrata nel campo `digestPublicKeyFingerprint` del file digest. Questa è la chiave pubblica che verrà utilizzata per convalidare il file digest.

D. Creazione di una nuova stringa di firma dei dati

Ora che disponi della firma del file digest e della chiave pubblica associata, devi calcolare la stringa di firma dei dati. Dopo aver calcolato tale stringa, si disporrà di tutte le informazioni necessarie per verificare la firma.

La stringa di firma dei dati ha il formato seguente:

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

Di seguito è riportato un esempio di stringa `Data_To_Sign_String`.

```
2015-08-12T04:01:31Z
amzn-s3-demo-bucket/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Dopo aver ricreato questa stringa, puoi convalidare il file digest.

E. Convalida del file digest

A questo punto puoi passare l'hash SHA-256 della stringa di firma dei dati ricreata, la firma digitale e la chiave pubblica all'algoritmo RSA di verifica della firma. Se l'output è true, la firma del file digest è verificata e il file digest è valido.

F. Convalida dei file di log

Dopo aver convalidato il file digest, puoi convalidare il file di log a cui fa riferimento. Il file digest contiene gli hash SHA-256 dei file di log. Se uno dei file di registro è stato modificato dopo la CloudTrail consegna, gli hash SHA-256 cambieranno e la firma del file digest non corrisponderà.

Di seguito è descritto come convalidare i file di log:

1. Eseguire un comando `S3 Get` sul file di log utilizzando le informazioni sulla posizione S3 nei campi `logFiles.s3Bucket` e `logFiles.s3Object` del file digest.
2. Se l'operazione `S3 Get` ha esito positivo, ripetere l'operazione nei file di log elencati nella matrice logFiles del file digest utilizzando la procedura seguente:
   a. Recuperate il valore hash originale del file dal campo `logFiles.hashValue` del log corrispondente nel file digest.
   b. Eseguire l'hashing dei contenuti non compressi del file di log con l'algoritmo di hashing specificato in `logFiles.hashAlgorithm`.
   c. Confrontare il valore hash generato con quello del log nel file digest. Se i valori hash corrispondono, il file di log è valido.

G. Convalida di file digest e file di log aggiuntivi

In ogni file digest, i seguenti campi forniscono le informazioni su posizione e firma del file digest precedente:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Utilizzare queste informazioni per recuperare i file digest precedenti in sequenza, convalidare la firma di ciascuno di essi e i file di log a cui fanno riferimento mediante le procedure descritta nelle sezioni precedenti. L'unica differenza risiede nel fatto che, per i file digest precedenti, non devi recuperare la firma digitale dalle proprietà metadati Amazon S3 dell'oggetto file digest. La firma del file digest precedente è disponibile automaticamente nel campo `previousDigestSignature`.

Puoi andare a ritroso nel tempo finché non raggiungi il file digest iniziale o fino all'interruzione della sequenza di file digest, a seconda di quale evento si verifica prima.

Convalida di file digest e file di log offline

Durante la convalida di file digest e file di log offline, in genere puoi fare riferimento alle procedure descritte nelle sezioni precedenti. Devi tuttavia tenere in considerazione i seguenti punti:

Utilizzo del file digest più recente

La firma digitale del file digest più recente (ovvero "corrente") si trova nelle proprietà metadati Amazon S3 dell'oggetto file digest. In uno scenario offline, la firma digitale del file digest corrente non sarà disponibile.

Per gestire questa situazione sono disponibili due modi:

- Poiché la firma digitale per il file digest precedente si trova nel file digest corrente, iniziate la convalida dal file digest. next-to-last Con questo metodo il file digest più recente non può essere convalidato.
- Come prima cosa recupera la firma del file digest corrente dalle proprietà metadati dell'oggetto del file digest e quindi memorizzala in modo sicuro offline. In questo modo il file digest corrente verrà convalidato assieme ai file precedenti nella sequenza.

Risoluzione del percorso

I campi nei file digest scaricati, ad esempio `s3Object` e `previousDigestS3Object`, continueranno a fare riferimento alle posizioni Amazon S3 online dei file di log e file digest. Una soluzione offline deve trovare un modo per reindirizzare queste posizioni al percorso corrente dei file di log e file digest scaricati.

Chiavi pubbliche

Per eseguire la convalida offline, tutte le chiavi pubbliche necessarie per convalidare i file di log in un determinato intervallo di tempo devono prima essere recuperate online (chiamando `ListPublicKeys`, ad esempio) e quindi memorizzate in modo sicuro offline. Questo passaggio deve essere ripetuto ogni volta che si vuole convalidare altri file non compresi nell'intervallo di tempo iniziale specificato.

Esempio di frammento di codice di convalida

Il seguente frammento di esempio fornisce un codice scheletrico per la convalida dei file digest e di registro. CloudTrail Il codice di base non fa distinzione tra le modalità online/offline, ovvero si potrà a scegliere autonomamente se implementare il codice con o senza una connessione online ad AWS. L'implementazione suggerita usa i provider di sicurezza Java Cryptography Extension (JCE) e Bouncy Castle.

Il frammento di codice di esempio mostra:

- Come creare la stringa di firma dei dati utilizzata per convalidare la firma del file digest.
- Come verificare la firma del file digest.
- Come verificare gli hash del file di log.
- Una struttura di codice per convalidare una sequenza di file digest.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
```

```
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
 digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
 as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
 ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
 file. Also, the public key bytes
```

```
                returned from ListPublicKey API are DER encoded in PKCS#1 format:

                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
```

```
                                            );
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
 Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail esempi di file di registro

CloudTrail monitora gli eventi relativi al tuo account. Se crei un percorso, esso distribuisce tali eventi sotto forma di file di log nel bucket Amazon S3. Se crei un archivio dati di eventi in CloudTrail Lake, gli eventi vengono registrati nel tuo archivio dati degli eventi. Gli archivi di dati degli eventi non utilizzano i bucket S3.

Argomenti

- CloudTrail formato del nome del file di registro
- Esempi di file di log

CloudTrail formato del nome del file di registro

CloudTrail utilizza il seguente formato di nome file per gli oggetti dei file di log che distribuisce al tuo bucket Amazon S3:

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- `YYYY`, `MM`, `DD`, `HH` e `mm` rappresentano i valori relativi ad anno, mese, giorno, ora e minuti che fanno riferimento alla data/ora di distribuzione del file di log. Le ore sono in formato 24 ore. Il valore `Z` indica che il tempo è in formato UTC.

  > **Note**
  >
  > Un file di log distribuito in un orario specifico può contenere report scritti in un momento qualsiasi prima di quell'orario.

- Il componente `UniqueString` a 16 caratteri del nome del file di log serve a impedire che i file vengano sovrascritti. Non ha alcun significato e il software di elaborazione dei log dovrebbe ignorarlo.
- `FileNameFormat` è la codifica del file. Al momento, la codifica è `json.gz`, che è un file di testo JSON in formato gzip compresso.

Esempio di nome del file di CloudTrail log

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

Esempi di file di log

Un file di log contiene uno o più record. I seguenti esempi sono parti di log che mostrano i record relativi a un'azione che ha avviato la creazione di un file di log.

Per informazioni sui campi dei record CloudTrail degli eventi, vedereCloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.

Indice

- Esempi di EC2 log Amazon
- Esempi di log di IAM
- Esempio di codice di errore e log dei messaggi
- CloudTrail Esempio di registro degli eventi di Insights

Esempi di EC2 log Amazon

Amazon Elastic Compute Cloud (Amazon EC2) fornisce capacità di calcolo ridimensionabile in. Cloud AWS Puoi avviare server virtuali, configurare la sicurezza e le reti, nonché gestire l'archiviazione. Amazon EC2 può anche scalare rapidamente verso l'alto o verso il basso per gestire i cambiamenti nei requisiti o i picchi di popolarità, riducendo così la necessità di prevedere il traffico del server. Per ulteriori informazioni, consulta la Amazon EC2 User Guide.

L'esempio seguente mostra che un utente IAM di nome `Mateo` ha eseguito il aws ec2 start-instances comando per chiamare l' EC2 `StartInstances`azione Amazon per le istanze `i-EXAMPLE56126103cb` `ei-EXAMPLEaff4840c22`.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
```

```
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

L'esempio seguente mostra che un utente IAM di nome `Nikki` ha eseguito il aws ec2 stop-instances comando per chiamare l' EC2 `StopInstances`azione Amazon per arrestare due istanze.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
```

```
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

L'esempio seguente mostra che l'utente IAM denominato `Arnav` ha eseguito il comando aws ec2 create-key-pair per richiamare l'operazione `CreateKeyPair`. Nota che `responseElements` contengono un hash della coppia di chiavi e che hanno AWS rimosso il materiale della chiave.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Esempi di log di IAM

AWS Identity and Access Management (IAM) è un servizio web che consente di controllare in modo sicuro l'accesso alle AWS risorse. Con IAM, puoi gestire a livello centrale le autorizzazioni che controllano le risorse AWS a cui possono accedere gli utenti. Utilizza IAM per controllare chi è

autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Per ulteriori informazioni, consultare la Guida per l'utente IAM.

L'esempio seguente mostra che l'utente IAM denominato `Mary` ha eseguito il comando aws iam create-user per richiamare l'operazione `CreateUser` per creare un nuovo utente denominato `Richard`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
```

```
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


L'esempio seguente mostra che l'utente IAM denominato `Paulo` ha eseguito il comando aws iam add-user-to-group per richiamare l'operazione `AddUserToGroup` per aggiungere un utente denominato `Jane` al gruppo `Admin`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


L'esempio seguente mostra che l'utente IAM denominato `Saanvi` ha eseguito il comando aws iam create-role per richiamare l'operazione `CreateRole` per creare un ruolo.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Esempio di codice di errore e log dei messaggi

L'esempio seguente mostra che l'utente IAM denominato `Terry` ha eseguito il comando aws cloudtrail update-trail per chiamare l'operazione `UpdateTrail` per aggiornare un percorso denominato `myTrail2`, ma il nome del percorso non è stato trovato. Il log mostra questo errore negli elementi `errorCode` e `errorMessage`.


```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail Esempio di registro degli eventi di Insights

L'esempio seguente mostra un registro degli eventi di CloudTrail Insights. Un evento Insights è in realtà una coppia di eventi che segnano l'inizio e la fine di un periodo di attività insolita dell'API di gestione della scrittura o un periodo di attività di risposta di errore. Il campo `state` indica se l'evento è stato registrato all'inizio o alla fine del periodo di attività insolita. Il nome dell'evento,`UpdateInstanceInformation`, è lo stesso nome dell' AWS Systems Manager API per la quale sono CloudTrail stati analizzati gli eventi di gestione per determinare che si è verificata un'attività insolita. Sebbene gli eventi di inizio e fine abbiano valori `eventID` univoci, hanno anche un valore `sharedEventID` che viene utilizzato dalla coppia. L'evento Insights mostra il valore `baseline` o modello normale di attività, il valore `insight` o attività insolita media che ha attivato l'evento Insights di inizio e nell'evento di fine il valore `insight` per l'attività insolita media nel corso della durata dell'evento Insights. Per ulteriori informazioni su CloudTrail Insights, consulta[Lavorare con CloudTrail Insights](#).

```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
```

```
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

Utilizzo della libreria CloudTrail di elaborazione

La CloudTrail Processing Library è una libreria Java che fornisce un modo semplice per elaborare AWS CloudTrail i log. Fornisci dettagli di configurazione sulla coda CloudTrail SQS e scrivi codice per elaborare gli eventi. La CloudTrail Processing Library fa il resto. Esegue il polling della coda Amazon SQS, legge e analizza i messaggi in coda, CloudTrail scarica i file di registro, analizza gli eventi nei file di registro e passa gli eventi al codice come oggetti Java.

La CloudTrail Processing Library è altamente scalabile e tollerante ai guasti. Gestisce l'elaborazione parallela dei file di log in modo da consentirti di elaborare qualsiasi numero di log in base alle tue specifiche esigenze. Gestisce inoltre gli errori di rete correlati a timeout di rete e risorse non accessibili.

L'argomento seguente mostra come utilizzare la CloudTrail Processing Library per elaborare i CloudTrail log nei progetti Java.

La libreria viene fornita come progetto open source con licenza Apache, disponibile su:. GitHub https://github.com/aws/aws-cloudtrail-processing-library La libreria include il codice di esempio che puoi utilizzare come base per i tuoi progetti.

Argomenti

- Requisiti minimi
- Registri di elaborazione CloudTrail
- Argomenti avanzati
- Risorse aggiuntive

Requisiti minimi

Per utilizzare la CloudTrail Processing Library, è necessario disporre di quanto segue:

- AWS SDK per Java 1.11.830
- Java 1.8 (Java SE 8)

Registri di elaborazione CloudTrail

Per elaborare CloudTrail i log nell'applicazione Java:

1. Aggiungere la CloudTrail Processing Library al progetto
2. Configurazione della Processing Library CloudTrail
3. Implementazione del processore di eventi
4. Creazione di un'istanza ed esecuzione dell'executor di elaborazione

Aggiungere la CloudTrail Processing Library al progetto

Per utilizzare la CloudTrail Processing Library, aggiungila al classpath del tuo progetto Java.

Indice

- Aggiunta della libreria a un progetto Apache Ant
- Aggiunta della libreria a un progetto Apache Maven
- Aggiunta della libreria a un progetto Eclipse
- Aggiunta della libreria a un progetto IntelliJ

Aggiunta della libreria a un progetto Apache Ant

Per aggiungere la CloudTrail Processing Library a un progetto Apache Ant

1. Scarica o clona il codice sorgente della CloudTrail Processing Library da: GitHub
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Compila il file .jar dal codice sorgente come descritto in LEGGIMI:

   ```
   mvn clean install -Dgpg.skip=true
   ```

3. Copiare il file con estensione .jar risultante nel progetto e aggiungerlo al file `build.xml` del progetto. Per esempio:

   ```
   <classpath>
     <pathelement path="${classpath}"/>
     <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
   </classpath>
   ```

Aggiunta della libreria a un progetto Apache Maven

La CloudTrail Processing Library è disponibile per Apache Maven. È possibile aggiungerla al progetto scrivendo un'unica dipendenza nel file `pom.xml` del progetto.

Per aggiungere la CloudTrail Processing Library a un progetto Maven

- Aprire il file `pom.xml` del progetto Maven e aggiungere la seguente dipendenza:

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

Aggiunta della libreria a un progetto Eclipse

Per aggiungere la CloudTrail Processing Library a un progetto Eclipse

1. Scarica o clona il codice sorgente della CloudTrail Processing Library da: GitHub
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Compila il file .jar dal codice sorgente come descritto in LEGGIMI:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Copia il aws-cloudtrail-processing-library -1.6.1.jar creato in una directory del tuo progetto (in genere). `lib`
4. Fare clic con il pulsante destro del mouse sul nome del progetto nella finestra Project Explorer (Explorer progetti) di Eclipse, scegliere Build Path (Percorso di compilazione) e quindi scegliere Configure (Configura).
5. Nella finestra Java Build Path (Percorso di compilazione Java) scegliere la scheda Libraries (Librerie).
6. Scegli Aggiungi... JARs e vai al percorso in cui hai copiato aws-cloudtrail-processing-library -1.6.1.jar.
7. Scegliere OK per completare l'aggiunta del file `.jar` al progetto.

Aggiunta della libreria a un progetto IntelliJ

Per aggiungere la CloudTrail Processing Library a un progetto IntelliJ

1. Scarica o clona il codice sorgente della CloudTrail Processing Library da: GitHub
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Compila il file .jar dal codice sorgente come descritto in LEGGIMI:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. In File, scegliere Project Structure (Struttura progetto).
4. Scegliere Modules (Moduli), quindi Dependencies (Dipendenze).
5. Scegliere + JARS or Directories (+ File JAR o directory) e quindi passare al percorso di compilazione del file `aws-cloudtrail-processing-library-1.6.1.jar`.
6. Scegliere Apply (Applica) e quindi OK per completare l'aggiunta del file `.jar` al progetto.

Configurazione della Processing Library CloudTrail

È possibile configurare la CloudTrail Processing Library creando un file delle proprietà del percorso di classe che viene caricato in fase di esecuzione oppure creando un `ClientConfiguration` oggetto e impostando le opzioni manualmente.

Specificare un file delle proprietà

Puoi scrivere un file delle proprietà del classpath per specificare le opzioni di configurazione da passare all'applicazione. Il file di esempio seguente mostra le opzioni che è possibile impostare:

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1
```

```
# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

I parametri seguenti sono obbligatori:

- `sqsUrl`— Fornisce l'URL da cui estrarre le CloudTrail notifiche. Se non specifichi questo valore, `AWSCloudTrailProcessingExecutor` restituisce un'eccezione `IllegalStateException`.
- `accessKey`— Un identificatore univoco per il tuo account, ad esempio AKIAIOSFODNN7EXAMPLE.
- `secretKey`— Un identificatore univoco per il tuo account, ad esempio wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

I `secretKey` parametri `accessKey` and forniscono AWS le credenziali dell'utente alla libreria, in modo che quest'ultima possa accedere per AWS conto dell'utente.

Le impostazioni di default per gli altri parametri vengono definite dalla libreria. Per ulteriori informazioni, consulta Documentazione di riferimento della libreria di elaborazione AWS CloudTrail.

Creare un ClientConfiguration

Anziché impostare le opzioni nelle proprietà del classpath, puoi specificare le opzioni per `AWSCloudTrailProcessingExecutor` mediante l'inizializzazione e l'impostazione delle opzioni in un oggetto `ClientConfiguration`, come illustrato nel seguente esempio:

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

Implementazione del processore di eventi

Per elaborare CloudTrail i registri, è necessario implementare un file `EventsProcessor` che riceva i dati di CloudTrail registro. Di seguito è riportato un esempio di implementazione:

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

Quando si implementa un`EventsProcessor`, si implementa il `process()` callback che `AWSCloudTrailProcessingExecutor` utilizza per inviarti CloudTrail eventi. Gli eventi vengono forniti in un elenco di oggetti `CloudTrailClientEvent`.

L'`CloudTrailClientEvent`oggetto fornisce un `CloudTrailEvent` e `CloudTrailEventMetadata` che è possibile utilizzare per leggere le informazioni sull' CloudTrail evento e sulla consegna.

Questo semplice esempio stampa le informazioni sugli eventi per ogni evento passato a `SampleEventsProcessor`. Nell'ambito dell'implementazione in questione puoi elaborare i log in base alle specifiche esigenze di lavoro. L'oggetto `AWSCloudTrailProcessingExecutor` continua

a inviare gli eventi all'oggetto `EventsProcessor` a condizione che disponga di eventi da inviare e che sia ancora in esecuzione.

Creazione di un'istanza ed esecuzione dell'executor di elaborazione

Dopo aver scritto `EventsProcessor` e impostato i valori di configurazione per la CloudTrail Processing Library (in un file di proprietà o utilizzando la `ClientConfiguration` classe), potete utilizzare questi elementi per inizializzare e utilizzare un`AWSCloudTrailProcessingExecutor`.

Da utilizzare **`AWSCloudTrailProcessingExecutor`** per elaborare eventi CloudTrail

1. Creare un'istanza di un oggetto `AWSCloudTrailProcessingExecutor.Builder`. Il costruttore di `Builder`richiede un oggetto `EventsProcessor` e un nome di file delle proprietà del classpath.
2. Chiamare il metodo factory `build()` di `Builder` per configurare e recuperare un oggetto `AWSCloudTrailProcessingExecutor`.
3. Usa i `AWSCloudTrailProcessingExecutor` `stop()` metodi `start()` e per iniziare e terminare CloudTrail l'elaborazione degli eventi.

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

Argomenti avanzati

Argomenti

- Filtro degli eventi da elaborare
- Elaborazione di eventi di dati
- Creazione di report sull'avanzamento
- Gestione degli errori

Filtro degli eventi da elaborare

Per impostazione predefinita, tutti i log nel bucket S3 della coda Amazon SQS e tutti gli eventi in esso contenuti vengono inviati a `EventsProcessor`. La CloudTrail Processing Library fornisce interfacce opzionali che è possibile implementare per filtrare le fonti utilizzate per ottenere CloudTrail i log e per filtrare gli eventi che si desidera elaborare.

`SourceFilter`

Puoi implementare l'interfaccia `SourceFilter` per scegliere se elaborare i log provenienti dall'origine specificata. `SourceFilter` dichiara un singolo metodo di callback, `filterSource()`, che riceve un oggetto `CloudTrailSource`. Per evitare che gli eventi provenienti da un'origine vengano elaborati, impostare la restituzione di `false` da `filterSource()`.

La CloudTrail Processing Library chiama il `filterSource()` metodo dopo che la libreria ha effettuato il polling dei log sulla coda Amazon SQS. Ciò si verifica prima che la libreria inizi il filtraggio degli eventi o l'elaborazione dei log.

Di seguito è riportato un esempio di implementazione:

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());
```

```
    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

Se non specifichi l'interfaccia `SourceFilter`, viene utilizzato `DefaultSourceFilter`, che permette l'elaborazione di tutte le origini (restituirà sempre `true`).

`EventFilter`

Puoi implementare l'interfaccia `EventFilter` per scegliere se un evento CloudTrail viene inviato a `EventsProcessor`. `EventFilter` dichiara un singolo metodo di callback, `filterEvent()`, che riceve un oggetto `CloudTrailEvent`. Per evitare che l'evento venga elaborato, impostare la restituzione di `false` da `filterEvent()`.

La CloudTrail Processing Library chiama il `filterEvent()` metodo dopo che la libreria ha effettuato il polling dei log sulla coda di Amazon SQS e dopo il filtraggio del codice sorgente. Ciò si verifica prima che la libreria inizi l'elaborazione dei log.

Di seguito è riportato un esempio di implementazione:

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

Se non specifichi l'interfaccia `EventFilter`, viene utilizzato `DefaultEventFilter`, che permette l'elaborazione di tutti gli eventi (restituirà sempre `true`).

Elaborazione di eventi di dati

Quando CloudTrail elabora gli eventi relativi ai dati, conserva i numeri nel loro formato originale, sia esso un numero intero (`int`) o un (un numero che contiene un `float` decimale). Negli eventi che contengono numeri interi nei campi di un evento di dati, CloudTrail storicamente elaborava questi numeri come float. Attualmente, CloudTrail elabora i numeri in questi campi mantenendo il formato originale.

Come best practice, per evitare di interrompere le automazioni, sii flessibile in qualsiasi codice o automazione che utilizzi per elaborare o filtrare gli eventi CloudTrail relativi ai dati e consenti sia `int` i `float` numeri formattati che i numeri. Per ottenere risultati ottimali, utilizzate la versione 1.4.0 o successiva della Processing Library. CloudTrail

L'esempio di frammento seguente mostra un numero formattato come `float`,`2.0`, per il parametro `desiredCount` nel blocco `ResponseParameters` di un evento di dati.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

L'esempio di frammento seguente mostra un numero formattato come `int`,2, per il parametro `desiredCount` nel blocco `ResponseParameters` di un evento di dati.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

Creazione di report sull'avanzamento

Implementa l'`ProgressReporter`interfaccia per personalizzare la segnalazione dei progressi della CloudTrail Processing Library. `ProgressReporter`dichiara due metodi: `reportStart()` e`reportEnd()`, che vengono chiamati all'inizio e alla fine delle seguenti operazioni:

- Polling dei messaggi da Amazon SQS
- Analisi dei messaggi da Amazon SQS
- Elaborazione di un codice sorgente Amazon SQS per i log CloudTrail
- Eliminazione dei messaggi da Amazon SQS
- Scaricamento di un file di registro CloudTrail
- Elaborazione di un file di CloudTrail registro

Entrambi i metodi ricevono un oggetto `ProgressStatus` contenente le informazioni sull'operazione eseguita. Il membro `progressState` contiene un membro dell'enumerazione `ProgressState` che identifica l'operazione corrente. Questo utente può contenere ulteriori informazioni sul membro `progressInfo`. Inoltre, qualsiasi oggetto restituito da `reportStart()` viene passato a `reportEnd()`. In questo modo puoi fornire informazioni contestuali, ad esempio l'ora di inizio dell'elaborazione dell'evento.

Di seguito è riportata un'implementazione di esempio che fornisce informazioni sul tempo richiesto per il completamento di un'operazione:

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
```

```
}
```

Se non implementi l'interfaccia `ProgressReporter`, viene utilizzato `DefaultExceptionHandler`, che stampa il nome dello stato in esecuzione.

Gestione degli errori

L'interfaccia `ExceptionHandler` ti consente di implementare una funzionalità di gestione speciale quando si verifica un'eccezione durante l'elaborazione dei log. `ExceptionHandler` dichiara un singolo metodo di callback, `handleException()`, che riceve un oggetto `ProcessingLibraryException` contenente il contesto relativo all'eccezione verificata.

Puoi utilizzare il metodo `getStatus()` dell'oggetto `ProcessingLibraryException` passato per scoprire quale operazione è stata eseguita quando si è verificata l'eccezione e per recuperare ulteriori informazioni sullo stato dell'operazione. L'oggetto `ProcessingLibraryException` è derivato dalla classe Java standard `Exception`. Puoi pertanto recuperare informazioni sull'eccezione anche richiamando qualsiasi metodo dell'eccezione.

Di seguito è riportato un esempio di implementazione:

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

Se non specifichi l'interfaccia `ExceptionHandler`, viene utilizzato `DefaultExceptionHandler`, che stampa un messaggio di errore standard.

> **Note**
>
> Se il `deleteMessageUponFailure` parametro è`true`, la CloudTrail Processing Library non distingue le eccezioni generali dagli errori di elaborazione e può eliminare i messaggi in coda.
>
> 1. Ad esempio, utilizzare `SourceFilter` per filtrare i messaggi in base al time stamp.
> 2. Tuttavia, non disponi delle autorizzazioni necessarie per accedere al bucket S3 che riceve i file di registro. CloudTrail Poiché non si dispone delle autorizzazioni necessarie, viene generata un'eccezione `AmazonServiceException`. La CloudTrail Processing Library lo racchiude in un. `CallBackException`
> 3. `DefaultExceptionHandler` registra questa situazione come un errore, ma non ne identifica la causa, ovvero che non si dispone delle autorizzazioni necessarie. La CloudTrail Processing Library lo considera un errore di elaborazione ed elimina il messaggio, anche se il messaggio include un file di registro valido CloudTrail .
>
> Se si desidera filtrare i messaggi con `SourceFilter`, verificare che `ExceptionHandler` sia in grado di distinguere le eccezioni del servizio dagli errori di elaborazione.

Risorse aggiuntive

Per ulteriori informazioni sulla CloudTrail Processing Library, vedere quanto segue:

- CloudTrail GitHub Progetto Processing Library, che include un codice di esempio che dimostra come implementare un'applicazione CloudTrail Processing Library.
- CloudTrail Documentazione del pacchetto Java della libreria di elaborazione.

Sicurezza in AWS CloudTrail

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di 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. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS CloudTrail, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo CloudTrail. I seguenti argomenti mostrano come eseguire la configurazione CloudTrail per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere CloudTrail le tue risorse.

Argomenti

- Protezione dei dati in AWS CloudTrail
- Identity and Access Management per AWS CloudTrail
- Convalida della conformità per AWS CloudTrail
- Resilienza in AWS CloudTrail
- Sicurezza dell'infrastruttura in AWS CloudTrail
- Prevenzione del problema "confused deputy" tra servizi
- Le migliori pratiche di sicurezza in AWS CloudTrail
- Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS)

Protezione dei dati in AWS CloudTrail

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS CloudTrail. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l' Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la registrazione dell'API e delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza le soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza di default all'interno dei Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-3 quando si accede ad AWS tramite un'interfaccia a riga di comando o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori CloudTrail o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Per impostazione predefinita, i file di log CloudTrail degli eventi e i file digest vengono crittografati utilizzando la crittografia lato server (SSE) di Amazon S3. Puoi anche scegliere di crittografare i file di log e i file digest con una chiave (). AWS Key Management Service AWS KMS Puoi archiviare i file di log nel tuo bucket per la durata desiderata. Puoi anche definire regole del ciclo di vita di Amazon S3 per archiviare o eliminare file di log automaticamente. Se desideri ricevere notifiche relative alla distribuzione e alla convalida dei file di log, puoi configurare le notifiche Amazon SNS.

Le best practice di sicurezza seguenti gestiscono anche la protezione dei dati in CloudTrail:

- Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS)
- Policy sui bucket Amazon S3 per CloudTrail
- Convalida dell'integrità dei file di CloudTrail registro
- Condivisione di file di CloudTrail registro tra AWS account

Poiché i file di CloudTrail log vengono archiviati in uno o più bucket in Amazon S3, dovrai esaminare anche le informazioni sulla protezione dei dati riportate nella Guida per l'utente di Amazon Simple Storage Service. Per ulteriori informazioni, consulta Protezione dei dati in Amazon S3.

Identity and Access Management per AWS CloudTrail

AWS Identity and Access Management (IAM) è un sistema Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. CloudTrail IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come AWS CloudTrail funziona con IAM
- Esempi di policy basate sull'identità per AWS CloudTrail
- AWS CloudTrail esempi di policy basate sulle risorse

- Policy sui bucket Amazon S3 per CloudTrail
- Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake
- Policy tematica di Amazon SNS per CloudTrail
- Risoluzione dei problemi relativi AWS CloudTrail all'identità e all'accesso
- Utilizzo di ruoli collegati ai servizi per CloudTrail
- AWS politiche gestite per AWS CloudTrail

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che CloudTrail svolgi.

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

Amministratore del servizio: se sei responsabile delle CloudTrail risorse della tua azienda, probabilmente hai pieno accesso a CloudTrail. È tuo compito determinare a quali CloudTrail funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con CloudTrail, consultaCome AWS CloudTrail funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a CloudTrail. Per visualizzare esempi di policy CloudTrail basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per AWS CloudTrail

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

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

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

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

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

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

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

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o

utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

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

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

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

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

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

Policy basate sulle risorse

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

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

Liste di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come AWS CloudTrail funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a CloudTrail, scopri con quali funzionalità IAM è possibile utilizzare CloudTrail.

Funzionalità IAM che puoi utilizzare con AWS CloudTrail

Funzionalità IAM	CloudTrail supporto
Policy basate su identità	Sì
Policy basate su risorse	Parziale
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	No
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come CloudTrail e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per CloudTrail

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per CloudTrail

Per visualizzare esempi di politiche basate sull' CloudTrail identità, vedere. Esempi di policy basate sull'identità per AWS CloudTrail

Politiche basate sulle risorse all'interno CloudTrail

Supporta politiche basate sulle risorse: parziale

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

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

CloudTrail supporta i seguenti tipi di politiche basate sulle risorse:

- Politiche basate sulle risorse sui canali utilizzati per le integrazioni di CloudTrail Lake con fonti di eventi esterne a. AWS La policy basata sulle risorse per il canale definisce quali entità principali (account, utenti, ruoli e utenti federati) possono chiamare `PutAuditEvents` sul canale per distribuire gli eventi all'archivio di dati degli eventi di destinazione. Per ulteriori informazioni sulla creazione di integrazioni con Lake, consulta. CloudTrail Crea un'integrazione con una fonte di eventi esterna a AWS
- Policy basate sulle risorse per controllare quali responsabili possono eseguire azioni sul data store degli eventi. Puoi utilizzare politiche basate sulle risorse per fornire l'accesso tra più account ai tuoi archivi di dati di eventi.
- Politiche basate sulle risorse sulle dashboard per consentire l'aggiornamento di una dashboard di CloudTrail Lake CloudTrail all'intervallo definito quando imposti una pianificazione di aggiornamento per una dashboard. Per ulteriori informazioni, consulta Imposta una pianificazione di aggiornamento per una dashboard personalizzata con la console CloudTrail .

Esempi

Per visualizzare esempi di politiche basate sulle risorse, consulta. CloudTrail AWS CloudTrail esempi di policy basate sulle risorse

Azioni politiche per CloudTrail

Supporta le operazioni di policy: si

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

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione

AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Per visualizzare un elenco di CloudTrail azioni, vedere Azioni definite da AWS CloudTrail nel Service Authorization Reference.

Le azioni politiche in CloudTrail uso utilizzano il seguente prefisso prima dell'azione:

```
cloudtrail
```

Ad esempio, per concedere a qualcuno l'autorizzazione a elencare i tag per un trial con l'operazione API `ListTags`, includere l'operazione `cloudtrail:ListTags` nella policy. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. CloudTrail definisce un proprio set di operazioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

Puoi specificare più operazioni tramite caratteri jolly (`*`). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Get`, includi la seguente azione:

```
"Action": "cloudtrail:Get*"
```

Risorse politiche per CloudTrail

Supporta le risorse di policy: sì

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

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

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

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

Per visualizzare un elenco dei tipi di CloudTrail risorse e relativi ARNs, vedere Resources Defined by AWS CloudTrail nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da AWS CloudTrail.

Esistono quattro tipi di risorse: percorsi, archivi di dati di eventi, dashboard e canali. CloudTrail A ogni risorsa è associato un Amazon Resource Name (ARN) univoco. In una policy, si utilizza un ARN per identificare la risorsa a cui si applica la policy. CloudTrail attualmente non supporta altri tipi di risorse, a volte denominate sottorisorse.

La risorsa CloudTrail trail ha il seguente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

La risorsa CloudTrail Event Data Store ha il seguente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

La risorsa del CloudTrail dashboard ha il seguente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/{DashboardName}
```

La risorsa del CloudTrail canale ha il seguente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

Per ulteriori informazioni sul formato di ARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Ad esempio, per un Account AWS con ID*123456789012*, per specificare nella dichiarazione un percorso denominato *My-Trail* che esiste nella regione Stati Uniti orientali (Ohio), utilizza il seguente ARN:

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Per specificare tutti i percorsi che appartengono a un account specifico Regione AWS, usa il carattere jolly (*):

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

Alcune CloudTrail azioni, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (`*`).

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

Molte azioni CloudTrail API coinvolgono più risorse. Ad esempio, `CreateTrail` richiede un bucket Amazon S3 per archiviare i file di log, pertanto un utente IAM dovrà disporre delle autorizzazioni di scrittura per il bucket. Per specificare più risorse in una singola istruzione, separale ARNs con virgole.

```
"Resource": [
      "resource1",
      "resource2"
```

Chiavi relative alle condizioni della politica per CloudTrail

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

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

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione

logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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

CloudTrail non definisce le proprie chiavi di condizione, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella IAM User Guide.

Per visualizzare un elenco di chiavi di CloudTrail condizione, consulta Condition Keys for AWS CloudTrail nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS CloudTrail.

ACLs in CloudTrail

Supporti ACLs: no

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

ABAC con CloudTrail

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

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

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

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Puoi allegare tag alle CloudTrail risorse o passarli in una richiesta a CloudTrail. Per ulteriori informazioni sull'etichettatura CloudTrail delle risorse, consulta Creazione di un percorso con la CloudTrail console eCreazione, aggiornamento e gestione di percorsi con AWS CLI.

Utilizzo di credenziali temporanee con CloudTrail

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per CloudTrail

Supporta l'inoltro delle sessioni di accesso (FAS): sì

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

Ruoli di servizio per CloudTrail

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. CloudTrail Modifica i ruoli di servizio solo quando viene CloudTrail fornita una guida in tal senso.

Ruoli collegati ai servizi per CloudTrail

Supporta ruoli collegati ai servizi: Sì

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

CloudTrail supporta un ruolo collegato al servizio per l'integrazione con. AWS Organizations Questo ruolo è necessario per la creazione di un percorso dell'organizzazione o di un datastore di eventi. I percorsi organizzativi e gli archivi dati degli eventi registrano gli eventi per tutti i membri Account AWS di un'organizzazione. Per ulteriori informazioni sulla creazione o la gestione di ruoli CloudTrail collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per CloudTrail

Esempi di policy basate sull'identità per AWS CloudTrail

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

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da CloudTrail, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione AWS CloudTrail nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Esempio: permettere e negare operazioni per un percorso specifico
- Esempi: creazione e applicazione di policy per le operazioni su percorsi specifici
- Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag
- Utilizzo della console di CloudTrail
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Concessione di autorizzazioni personalizzate per gli utenti CloudTrail

Best practice per le policy

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

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

CloudTrail non dispone di chiavi contestuali specifiche del servizio che è possibile utilizzare nell'elemento delle `Condition` dichiarazioni politiche.

Esempio: permettere e negare operazioni per un percorso specifico

L'esempio seguente illustra una politica che consente agli utenti che dispongono della policy di visualizzare lo stato e la configurazione di un itinerario e di avviare e interrompere la registrazione per un percorso denominato. *`My-First-Trail`* Questo percorso è stato creato nella regione degli Stati Uniti orientali (Ohio) (la sua regione di origine) Account AWS con l'ID. *`123456789012`*

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

L'esempio seguente mostra una politica che nega esplicitamente le CloudTrail azioni per qualsiasi percorso non denominato. *My-First-Trail*

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

Esempi: creazione e applicazione di policy per le operazioni su percorsi specifici

È possibile utilizzare autorizzazioni e policy per controllare la capacità di un utente di eseguire azioni specifiche sui sentieri. CloudTrail

Ad esempio, non vuoi che gli utenti del gruppo di sviluppatori della tua azienda avviino o arrestino la registrazione su un determinato percorso. Tuttavia, potresti voler concedere loro l'autorizzazione a eseguire le azioni `DescribeTrails` e `GetTrailStatus` lungo il percorso. Vuoi che gli utenti del gruppo di sviluppatori possano eseguire l'operazione `StartLogging` o `StopLogging` sui trail che gestiscono.

Puoi creare due istruzioni di policy e quindi collegarle al gruppo di sviluppatori creato in IAM. Per ulteriori informazioni sui gruppi in IAM, consulta Gruppi IAM nella Guida per l'utente di IAM.

Nella prima policy neghi l'autorizzazione per le operazioni `StartLogging` e `StopLogging` per l'ARN del trail specificato. Nell'esempio seguente, l'ARN del trail è `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

Nella seconda policy, le `GetTrailStatus` azioni `DescribeTrails` e sono consentite su tutte le CloudTrail risorse:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Se un utente del gruppo di sviluppatori cerca di avviare o arrestare la registrazione per il trail specificato nella prima policy, all'utente viene restituita un'eccezione di accesso negato. Gli utenti del gruppo di sviluppatori possono avviare e arrestare la registrazione per i trail che creano e gestiscono.

Gli esempi seguenti mostrano che il gruppo di sviluppatori configurato ha un AWS CLI profilo denominato`devgroup`. In primo luogo, un utente di `devgroup` esegue il comando `describe-trails`.

```
$ aws --profile devgroup cloudtrail describe-trails
```

Se il comando viene completato correttamente, l'output è il seguente:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
```

```
            "S3BucketName": "amzn-s3-demo-bucket",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

L'utente esegue quindi il comando `get-trail-status` sul trail specificato nella prima policy.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

Se il comando viene completato correttamente, l'output è il seguente:

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

Quindi, un utente nel gruppo `devgroup` esegue il comando `stop-logging` sullo stesso percorso.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

Il comando restituisce un'eccezione di accesso negato, come la seguente:

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

L'utente esegue il comando `start-logging` sullo stesso trail.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

Anche in questo caso il comando restituisce un'eccezione di accesso negato, come la seguente:

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

Esempi: diniego dell'accesso per creare o eliminare gli archivi di dati degli eventi in base ai tag

Nel seguente esempio di policy, l'autorizzazione per creare un datastore di eventi con `CreateEventDataStore` viene negata se almeno una delle seguenti condizioni non è soddisfatta:

- Il datastore di eventi non ha una chiave di tag di `stage` applicata a se stesso
- Il valore del tag stage non è `alpha`, `beta`, `gamma` o `prod`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
```

```
            }
        }
    ]
}
```

Nel seguente esempio di policy, l'autorizzazione per eliminare un datastore di eventi con `DeleteEventDataStore` viene negata se il datatore in questione ha il tag `stage` applicato con un valore di `prod`. Una policy simile può contribuire a proteggere un datastore di eventi dall'eliminazione accidentale.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Utilizzo della console di CloudTrail

Per accedere alla AWS CloudTrail console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle CloudTrail risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Concessione delle autorizzazioni per l'amministrazione CloudTrail

Per consentire ai ruoli o agli utenti IAM di amministrare una CloudTrail risorsa, come un percorso, un archivio dati di eventi o un canale, devi concedere autorizzazioni esplicite per eseguire le azioni associate alle attività. CloudTrail Nella maggior parte dei casi, puoi utilizzare una policy AWS gestita che contiene autorizzazioni predefinite.

> **Note**
>
> Le autorizzazioni concesse agli utenti per eseguire attività di CloudTrail amministrazione non sono le stesse autorizzazioni CloudTrail necessarie per inviare file di log ai bucket Amazon S3 o inviare notifiche ad argomenti di Amazon SNS. Per ulteriori informazioni su queste autorizzazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.
> Se configuri l'integrazione con Amazon CloudWatch Logs, richiede CloudTrail anche un ruolo che può assumere per fornire eventi a un gruppo di log di Amazon CloudWatch Logs. È necessario creare il ruolo che CloudTrail utilizza. Per ulteriori informazioni, consultare Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail e Invio di eventi ai registri CloudWatch .

Le seguenti politiche AWS gestite sono disponibili per CloudTrail:

- AWSCloudTrail_FullAccess— Questa policy fornisce l'accesso completo alle CloudTrail azioni sulle CloudTrail risorse, come percorsi, archivi di dati sugli eventi e canali. Questa politica fornisce le autorizzazioni necessarie per creare, aggiornare ed eliminare CloudTrail percorsi, archivi dati di eventi e canali.

  Questa policy fornisce anche le autorizzazioni per gestire il bucket Amazon S3, il gruppo di log CloudWatch per Logs e un argomento Amazon SNS per un trail. Tuttavia, la policy `AWSCloudTrail_FullAccess` gestita non fornisce le autorizzazioni per eliminare il bucket Amazon S3, il gruppo di log CloudWatch per Logs o un argomento di Amazon SNS. Per informazioni sulle politiche gestite per altri Servizi AWS, consulta la Managed Policy Reference Guide AWS .

  > **Note**
  >
  > La AWSCloudTrail_FullAccesspolicy non è pensata per essere condivisa su larga scala tra i tuoi Account AWS. Gli utenti con questo ruolo hanno la possibilità di disattivare o riconfigurare le funzioni di auditing più sensibili e importanti negli Account AWS. Per questo

motivo, è necessario applicare questa policy solo agli amministratori degli account. È necessario controllare e monitorare attentamente l'uso di questa policy.

- AWSCloudTrail_ReadOnlyAccess— Questo criterio concede le autorizzazioni per visualizzare la CloudTrail console, inclusi gli eventi recenti e la cronologia degli eventi. Questa policy consente inoltre di visualizzare percorsi, datastore di eventi e canali esistenti. I ruoli e gli utenti con questa policy possono scaricare la cronologia degli eventi, ma non possono creare o aggiornare percorsi, datastore di eventi o canali.

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in: AWS IAM Identity Center

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Create a role for a third-party identity provider (federation) della Guida per l'utente IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina Create a role for an IAM user della Guida per l'utente IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente IAM.

Risorse aggiuntive

Per saperne di più sull'utilizzo di IAM per fornire alle identità, come utenti e ruoli, l'accesso alle risorse del tuo account, consulta la sezione Configurazione con IAM and Access management for AWS resources in the IAM User Guide.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Concessione di autorizzazioni personalizzate per gli utenti CloudTrail

CloudTrail le politiche concedono le autorizzazioni agli utenti con cui collabora. CloudTrail Se devi concedere autorizzazioni diverse agli utenti, puoi allegare una CloudTrail policy a un gruppo IAM o a un utente. Puoi modificare la policy in modo da includere o escludere autorizzazioni specifiche. Puoi anche creare policy personalizzate. Le policy sono documenti JSON che definiscono le operazioni che un utente può eseguire e le risorse su cui l'utente può eseguire tali operazioni. Per esempi specifici, consulta Esempio: permettere e negare operazioni per un percorso specifico e Esempi: creazione e applicazione di policy per le operazioni su percorsi specifici.

Indice

- Accesso in sola lettura
- Accesso completo ad
- Concessione dell'autorizzazione alla visualizzazione delle AWS Config informazioni sulla console CloudTrail
- Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail
- Informazioni aggiuntive

Accesso in sola lettura

L'esempio seguente mostra una politica che garantisce l'accesso in sola lettura ai percorsi. CloudTrail Questo è equivalente alla policy gestita AWSCloudTrail_ReadOnlyAccess. Questa policy consente di concedere agli utenti l'autorizzazione per visualizzare le informazioni contenute nei trail, ma non di creare o aggiornare i trail.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Nelle istruzioni della policy, l'elemento `Effect` specifica se le operazioni sono consentite o negate. L'elemento `Action` elenca le operazioni specifiche che l'utente è autorizzato a eseguire. L'`Resource`elemento elenca le AWS risorse su cui l'utente è autorizzato a eseguire tali azioni. Per le politiche che controllano l'accesso alle CloudTrail azioni, l'`Resource`elemento è in genere impostato su`*`, un carattere jolly che significa «tutte le risorse».

I valori nell'`Action`elemento corrispondono a quelli APIs supportati dai servizi. Le operazioni sono precedute da `cloudtrail:` a indicare che fanno riferimento alle operazioni CloudTrail . Puoi utilizzare il carattere jolly `*` nell'elemento `Action`, come negli esempi seguenti:

- `"Action": ["cloudtrail:*Logging"]`

  Ciò consente tutte le CloudTrail azioni che terminano con «Logging» (`StartLogging`,`StopLogging`).
- `"Action": ["cloudtrail:*"]`

  Ciò consente tutte le CloudTrail azioni, ma non le azioni per altri AWS servizi.
- `"Action": ["*"]`

  Ciò consente tutte le AWS azioni. Questa autorizzazione è adatta per un utente che funge da amministratore AWS per il tuo account.

La policy di sola lettura non concede autorizzazioni utente per le operazioni `CreateTrail`, `UpdateTrail`, `StartLogging` e `StopLogging`. Gli utenti associati a questa policy non saranno autorizzati a creare trail, aggiornare trai o attivare e disattivare la registrazione. Per l'elenco delle CloudTrail azioni, consulta l'AWS CloudTrail API Reference.

Accesso completo ad

L'esempio seguente mostra una politica che garantisce l'accesso completo a CloudTrail. Questo è equivalente alla policy gestita AWSCloudTrail_FullAccess. Concede agli utenti il permesso di eseguire tutte le CloudTrail azioni. Consente inoltre agli utenti di registrare gli eventi relativi ai dati in

Amazon S3 e AWS Lambda di gestire i file nei bucket Amazon S3, gestire il CloudWatch modo in cui Logs CloudTrail monitora gli eventi di registro e gestire gli argomenti di Amazon SNS nell'account a cui l'utente è associato.

> **Important**
>
> La AWSCloudTrail_FullAccesspolicy o le autorizzazioni equivalenti non sono pensate per essere condivise ampiamente tra i tuoi account. AWS Gli utenti con questo ruolo o un accesso equivalente hanno la possibilità di disabilitare o riconfigurare le funzioni di controllo più sensibili e importanti nei propri account. AWS Per questo motivo, questa policy deve essere applicata solo agli amministratori dell'account e l'utilizzo di questa policy deve essere strettamente controllato e monitorato.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-logging-bucket1*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Concessione dell'autorizzazione alla visualizzazione delle AWS Config informazioni sulla console CloudTrail

È possibile visualizzare le informazioni sull'evento sulla CloudTrail console, incluse le risorse correlate a tale evento. Per queste risorse, puoi scegliere l' AWS Config icona per visualizzare la sequenza temporale di quella risorsa nella AWS Config console. Allega questa politica ai tuoi

utenti per concedere loro l'accesso in sola lettura AWS Config . Tuttavia, la policy non concede l'autorizzazione per modificare le impostazioni in AWS Config.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

Per ulteriori informazioni, consulta Visualizzazione di risorse a cui viene fatto riferimento tramite AWS Config.

Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail

Puoi visualizzare e configurare la consegna degli eventi a CloudWatch Logs nella CloudTrail console se disponi di autorizzazioni sufficienti. Queste sono le autorizzazioni che potrebbero essere superiori a quelle concesse agli amministratori CloudTrail. Allega questa policy agli amministratori che configureranno e gestiranno CloudTrail l'integrazione con Logs. CloudWatch La politica non concede loro le autorizzazioni nei CloudTrail o nei CloudWatch Logs direttamente, ma concede invece le autorizzazioni necessarie per creare e configurare il ruolo che CloudTrail assumerà per fornire correttamente gli eventi al tuo gruppo Logs. CloudWatch

JSON

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

```
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

Per ulteriori informazioni, consulta Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs.

Informazioni aggiuntive

Per saperne di più sull'utilizzo di IAM per fornire alle identità, come utenti e ruoli, l'accesso alle risorse del tuo account, consulta Getting started e Access management for AWS resources nella IAM User Guide.

AWS CloudTrail esempi di policy basate sulle risorse

Questa sezione fornisce esempi di policy basate sulle risorse per dashboard, archivi di dati di eventi e canali CloudTrail Lake.

CloudTrail supporta i seguenti tipi di politiche basate sulle risorse:

- Politiche basate sulle risorse sui canali utilizzati per le integrazioni di CloudTrail Lake con fonti di eventi esterne a. AWS La policy basata sulle risorse per il canale definisce quali entità principali (account, utenti, ruoli e utenti federati) possono chiamare `PutAuditEvents` sul canale per distribuire gli eventi all'archivio di dati degli eventi di destinazione. Per ulteriori informazioni sulla creazione di integrazioni con Lake, consulta. CloudTrail Crea un'integrazione con una fonte di eventi esterna a AWS
- Policy basate sulle risorse per controllare quali responsabili possono eseguire azioni sul data store degli eventi. Puoi utilizzare politiche basate sulle risorse per fornire l'accesso tra più account ai tuoi archivi di dati di eventi.
- Politiche basate sulle risorse sulle dashboard per consentire l'aggiornamento di una dashboard di CloudTrail Lake CloudTrail all'intervallo definito quando imposti una pianificazione di

aggiornamento per una dashboard. Per ulteriori informazioni, consulta Imposta una pianificazione di aggiornamento per una dashboard personalizzata con la console CloudTrail .

Esempi:

- Esempi di policy basate sulle risorse per i canali
- Esempi di policy basate su risorse per archivi di dati di eventi
- Esempio di policy basata sulle risorse per un pannello di controllo

Esempi di policy basate sulle risorse per i canali

La policy basata sulle risorse per il canale definisce quali entità principali (account, utenti, ruoli e utenti federati) possono chiamare `PutAuditEvents` sul canale per distribuire gli eventi all'archivio di dati degli eventi di destinazione.

Le informazioni richieste per la policy dipendono dal tipo di integrazione.

- Per un'integrazione direzionale, CloudTrail richiede che la policy contenga il nome del Account AWS IDs partner e richiede l'immissione dell'ID esterno univoco fornito dal partner. CloudTrail aggiunge automaticamente la politica delle risorse del partner Account AWS IDs alla politica delle risorse quando si crea un'integrazione utilizzando la CloudTrail console. Consulta la documentazione del partner per scoprire come ottenere i Account AWS numeri richiesti per la policy.
- Per l'integrazione di una soluzione, è necessario specificare almeno un Account AWS ID come principale e, facoltativamente, inserire un ID esterno per evitare di creare confusione tra deputati.

Di seguito sono riportati i requisiti per la policy basata sulle risorse:

- La policy deve includere almeno un'istruzione. La policy può avere un massimo di 20 istruzioni.
- Ogni istruzione contiene almeno un principale. Un principale è un account, un utente, un ruolo o un utente federato. Un'istruzione può avere un massimo di 50 principali.
- L'ARN della risorsa definito nella policy deve corrispondere all'ARN del canale al quale è collegata la policy.
- La policy contiene una sola operazione: `cloudtrail-data:PutAuditEvents`

Il proprietario del canale può chiamare l'API `PutAuditEvents` sul canale, a meno che la policy non gli neghi l'accesso alla risorsa.

Argomenti

- Esempio: fornire l'accesso al canale ai principali
- Esempio: utilizzo di un ID esterno per evitare il problema "confused deputy"

Esempio: fornire l'accesso al canale ai principali

L'esempio seguente concede le autorizzazioni ai principali con e `arn:aws:iam::123456789012:root` per chiamare l' ARN`arn:aws:iam::111122223333:root`PutAuditEventsAPI sul CloudTrail canale con l'ARN. `arn:aws:iam::444455556666:root` `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Esempio: utilizzo di un ID esterno per evitare il problema "confused deputy"

L'esempio seguente utilizza un ID esterno per gestire e prevenire il problema confused deputy. Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione.

Il partner di integrazione crea l'ID esterno da utilizzare nella policy. Quindi, ti fornisce l'ID esterno come parte della creazione dell'integrazione. Il valore può essere qualsiasi stringa univoca, ad esempio una passphrase o un numero di account.

L'esempio concede le autorizzazioni ai principali con e per `arn:aws:iam::123456789012:root` chiamare l' ARNs`arn:aws:iam::111122223333:root`PutAuditEventsAPI sulla risorsa del CloudTrail canale se la chiamata all'`PutAuditEvents`API include il valore dell'ID esterno definito nella policy. `arn:aws:iam::444455556666:root`

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Esempi di policy basate su risorse per archivi di dati di eventi

Le politiche basate sulle risorse consentono di controllare quali responsabili possono eseguire azioni sul data store degli eventi.

È possibile utilizzare politiche basate sulle risorse per fornire l'accesso tra più account e consentire ai responsabili selezionati di interrogare l'archivio dati degli eventi, elencare e annullare le query e visualizzare i risultati delle query.

Per la dashboard di CloudTrail Lake, vengono utilizzate politiche basate sulle risorse per consentire di CloudTrail eseguire query sui data store degli eventi per compilare i dati per i widget della dashboard quando la dashboard viene aggiornata. CloudTrail Lake ti offre la possibilità di allegare una policy predefinita basata sulle risorse ai tuoi archivi di dati di eventi quando crei una dashboard personalizzata o abiliti la dashboard Highlights sulla console. CloudTrail

Le seguenti azioni sono supportate nelle politiche basate sulle risorse per gli archivi di dati di eventi:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Quando crei o aggiorni un data store di eventi o gestisci dashboard sulla CloudTrail console, hai la possibilità di aggiungere una policy basata sulle risorse al tuo archivio dati di eventi. Puoi anche eseguire il put-resource-policycomando per allegare una policy basata sulle risorse a un data store di eventi.

Una politica basata sulle risorse è costituita da una o più istruzioni. Ad esempio, può includere un'istruzione che consente CloudTrail di interrogare l'Event Data Store per un dashboard e un'altra istruzione che consente l'accesso a più account per interrogare l'Event Data Store. È possibile aggiornare la politica basata sulle risorse di un Event Data Store esistente dalla pagina dei dettagli dell'Event Data Store sulla console. CloudTrail

Per gli archivi dati degli eventi organizzativi, CloudTrail crea una politica predefinita basata sulle risorse che elenca le azioni che gli account amministratore delegati possono eseguire sui data store degli eventi organizzativi. Le autorizzazioni contenute in questa politica derivano dalle autorizzazioni di amministratore delegato in. AWS Organizations Questa politica viene aggiornata automaticamente in seguito alle modifiche all'archivio dati degli eventi dell'organizzazione o all'organizzazione (ad esempio, un account amministratore CloudTrail delegato viene registrato o rimosso).

Esempi:

- Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard
- Esempio: consenti ad altri account di interrogare un archivio dati di eventi e visualizzare i risultati delle query

Esempio: consenti CloudTrail di eseguire query per aggiornare una dashboard

Per compilare i dati su una dashboard di CloudTrail Lake durante un aggiornamento, devi consentire l'esecuzione di query CloudTrail per tuo conto. A tale scopo, allega una policy basata sulle risorse a ciascun archivio di dati di eventi associato a un widget del dashboard che include un'istruzione che consente CloudTrail di eseguire l'`StartQuery`operazione di compilazione dei dati per il widget.

Di seguito sono riportati i requisiti per la dichiarazione:

- L'unico `Principal` è`cloudtrail.amazonaws.com`.
- L'unico `Action` permesso è`cloudtrail:StartQuery`.
- Include `Condition` solo l'ARN (i) e Account AWS l'ID del dashboard. Infatti`AWS:SourceArn`, puoi fornire una serie di dashboard ARNs.

La seguente politica di esempio include un'istruzione che consente di CloudTrail eseguire query su un Event Data Store per due dashboard personalizzate denominate `example-dashboard1` and `example-dashboard2` e la dashboard Highlights denominata account`AWSCloudTrail-Highlights`. `123456789012`

JSON

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

```
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartQuery"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
               "StringLike": {
                  "AWS:SourceArn": [
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard1",
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard2",
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
AWSCloudTrail-Highlights"
                  ],
                  "AWS:SourceAccount": "123456789012"
               }
            }
        }
    ]
}
```

Esempio: consenti ad altri account di interrogare un archivio dati di eventi e visualizzare i risultati delle query

È possibile utilizzare politiche basate sulle risorse per fornire l'accesso tra più account agli archivi dati degli eventi per consentire ad altri account di eseguire query sui data store degli eventi.

La seguente politica di esempio include un'istruzione che consente agli utenti root degli account `111122223333` e di eseguire query e `111111111111` ottenere risultati di query sull'archivio dati degli eventi di proprietà dell'ID dell'account. `777777777777` `999999999999` `555555555555`

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "policy1",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::777777777777:root",
            "arn:aws:iam::999999999999:root",
            "arn:aws:iam::111111111111:root"
        ]
      },
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetQueryResults"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:555555555555:eventdatastore/
example80-699f-4045-a7d2-730dbf313ccf"
    }
  ]
}
```

Esempio di policy basata sulle risorse per un pannello di controllo

Puoi impostare una pianificazione di aggiornamento per una dashboard di CloudTrail Lake, che consente di CloudTrail aggiornare la dashboard per tuo conto all'intervallo definito quando imposti la pianificazione di aggiornamento. A tale scopo, è necessario allegare alla dashboard una policy basata sulle risorse che CloudTrail consenta di eseguire l'operazione sulla dashboard. `StartDashboardRefresh`

Di seguito sono riportati i requisiti per la policy basata sulle risorse:

- L'unico è. `Principal` `cloudtrail.amazonaws.com`
- L'unico `Action` permesso nella polizza è`cloudtrail:StartDashboardRefresh`.
- Include `Condition` solo l'ARN e Account AWS l'ID del pannello di controllo.

La seguente politica di esempio consente CloudTrail di aggiornare una dashboard denominata account`exampleDash`. `123456789012`

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartDashboardRefresh"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash",
                    "AWS:SourceAccount":"123456789012"
                }
            }
        }
    ]
}
```

Policy sui bucket Amazon S3 per CloudTrail

Per impostazione predefinita, i bucket e gli oggetti Amazon S3 sono privati. Solo il proprietario della risorsa (l'account AWS che ha creato il bucket) può accedere al bucket e agli oggetti in esso contenuti. Il proprietario della risorsa può concedere le autorizzazioni di accesso ad altre risorse e ad altri utenti mediante una policy di accesso.

Per creare o modificare un bucket Amazon S3 per ricevere file di log per un percorso dell'organizzazione, devi cambiare la policy del bucket. Per ulteriori informazioni, consulta Creare un percorso per un'organizzazione con AWS CLI.

Per inviare i file di registro a un bucket S3, è CloudTrail necessario disporre delle autorizzazioni richieste e il bucket non può essere configurato come bucket Requester Pays.

CloudTrail aggiunge automaticamente i seguenti campi nella politica:

- I consentiti SIDs
- Nome del bucket
- Il nome principale del servizio per CloudTrail
- Il nome della cartella in cui sono archiviati i file di registro, incluso il nome del bucket, un prefisso (se ne hai specificato uno) e l'ID dell'account AWS

Come best practice per la sicurezza, aggiungere una chiave di condizione `aws:SourceArn` per la policy del bucket Amazon S3. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la CloudTrail scrittura nel bucket S3 sia valida solo per uno o più percorsi specifici. Il valore di `aws:SourceArn` è sempre l'ARN del percorso (o dell'array di percorsi ARNs) che utilizza il bucket per archiviare i log. Assicurarsi di aggiungere la chiave di condizione `aws:SourceArn` alle politiche del bucket S3 per i percorsi esistenti.

> **Note**
>
> Se configuri male il percorso (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterà di reinviare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti ai costi standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

La seguente politica consente di scrivere file di registro nel bucket CloudTrail da Supported. Regioni AWS Sostituisci *`amzn-s3-demo-bucket[optionalPrefix]/`*,*`myAccountID`*,*`region`*, e *`trailName`* con i valori appropriati per la tua configurazione.

Policy del bucket S3

JSON

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

```
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni su Regioni AWS, vedereCloudTrail Regioni supportate.

Indice

- Specificare un bucket esistente per CloudTrail la consegna dei log
- Ricezione di file di log da altri account
- Creazione o aggiornamento di un bucket Amazon S3 da utilizzare per archiviare i file di log per un percorso dell'organizzazione
- Risoluzione dei problemi della policy del bucket Amazon S3
  - Errori di configurazione comuni della policy Amazon S3
  - Modifica di un prefisso per un bucket esistente

- Risorse aggiuntive

Specificare un bucket esistente per CloudTrail la consegna dei log

Se hai specificato un bucket S3 esistente come posizione di archiviazione per la consegna dei file di registro, devi allegare una policy al bucket che CloudTrail consenta di scrivere nel bucket.

> **Note**
>
> Come best practice, usa un bucket S3 dedicato per i log. CloudTrail

Per aggiungere la CloudTrail policy richiesta a un bucket Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Scegli il bucket in cui desideri distribuire CloudTrail i file di registro, quindi scegli Autorizzazioni.
3. Scegliere Edit (Modifica).
4. Copiare la S3 bucket policy nella finestra Bucket Policy Editor (Editor policy bucket). Sostituire i segnaposto in corsivo con i nomi per il bucket, il prefisso e il numero di account. Se è stato specificato un prefisso durante la creazione del trail, includerlo qui. Il prefisso è un'aggiunta opzionale alla chiave dell'oggetto S3 che crea un'organizzazione con stile cartella nel tuo bucket.

   > **Note**
   >
   > Se il bucket esistente ha già una o più politiche allegate, aggiungi le istruzioni per l' CloudTrail accesso a quella o alle politiche. Valutare il set di autorizzazioni risultante per accertarsi che siano appropriate per gli utenti che accedono al bucket.

Ricezione di file di log da altri account

Puoi CloudTrail configurare la distribuzione dei file di registro da più AWS account a un singolo bucket S3. Per ulteriori informazioni, consulta Ricezione di file di CloudTrail registro da più account.

Creazione o aggiornamento di un bucket Amazon S3 da utilizzare per archiviare i file di log per un percorso dell'organizzazione

Devi specificare un bucket Amazon S3 per ricevere i file di log per un percorso dell'organizzazione. Questo bucket deve avere una politica che CloudTrail consenta di inserire i file di registro dell'organizzazione nel bucket.

Di seguito è riportato un esempio di policy per un bucket Amazon S3 denominato*amzn-s3-demo-bucket*, di proprietà dell'account di gestione dell'organizzazione. Sostituisci *amzn-s3-demo-bucketregion*,*managementAccountID*,*trailName*, e *o-organizationID* con i valori della tua organizzazione

Questa policy del bucket contiene tre istruzioni.

- La prima istruzione consente di CloudTrail richiamare l'`GetBucketAcl`azione Amazon S3 sul bucket Amazon S3.
- La seconda istruzione consente la registrazione nel caso in cui il percorso venga modificato da percorso dell'organizzazione a percorso solo per quell'account.
- La terza istruzione consente la registrazione di un percorso dell'organizzazione.

Il criterio di esempio include una chiave di condizione `aws:SourceArn` per la policy del bucket Amazon S3. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la CloudTrail scrittura nel bucket S3 sia valida solo per uno o più percorsi specifici. In un trail dell'organizzazione, il valore di `aws:SourceArn` deve essere un ARN trail di proprietà dell'account di gestione e utilizza l'ID dell'account di gestione.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
```

```
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/
AWSLogs/managementAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/AWSLogs/o-
organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
```

```
                }
            }
        }
    ]
}
```

Questa policy di esempio non consente agli utenti degli account membri di accedere ai file di log creati per l'organizzazione. Per impostazione predefinita, i file di log dell'organizzazione sono accessibili solo per l'account di gestione. Per informazioni su come permettere l'accesso in lettura al bucket Amazon S3 per gli utenti IAM degli account membri, consulta Condivisione di file di CloudTrail registro tra AWS account.

Risoluzione dei problemi della policy del bucket Amazon S3

Le seguenti sezioni descrivono come risolvere i problemi relativi alla policy del bucket S3.

> **Note**
>
> Se configuri erroneamente il trail (ad esempio, il bucket S3 non è raggiungibile), CloudTrail tenterà di reinviare i file di registro al bucket S3 per 30 giorni e questi eventi saranno soggetti ai costi standard. attempted-to-deliver CloudTrail Per evitare addebiti su un percorso configurato erroneamente devi eliminarlo.

Errori di configurazione comuni della policy Amazon S3

Quando crei un nuovo bucket durante il processo di creazione o aggiornamento di un trail, CloudTrail collega le autorizzazioni necessarie al bucket. La policy del bucket utilizza il nome principale del servizio, che consente di fornire log per tutte le `"cloudtrail.amazonaws.com"` regioni. CloudTrail

Se non fornisce i log per una regione, CloudTrail è possibile che il bucket abbia una politica precedente che specifica CloudTrail l'account per ogni regione. IDs Questa politica CloudTrail autorizza la consegna dei log solo per le regioni specificate.

Come procedura ottimale, aggiorna la politica per utilizzare un'autorizzazione con il responsabile del CloudTrail servizio. A tale scopo, sostituisci l'ID dell'account ARNs con il nome principale del servizio:`"cloudtrail.amazonaws.com"`. Ciò consente CloudTrail di fornire registri per le regioni attuali e nuove. Come best practice per la sicurezza, aggiungi una chiave di

condizione `aws:SourceArn` o `aws:SourceAccount` per la policy del bucket Amazon S3. Ciò consente di impedire l'accesso non autorizzato all'account al bucket S3. Se hai percorsi esistenti, assicurati di aggiungere una o più chiavi di condizione. Di seguito è riportato l'esempio di configurazione consigliata della policy. Sostituisci *amzn-s3-demo-bucket[optionalPrefix]/*,*myAccountID*,*region*, e *trailName* con i valori appropriati per la tua configurazione.

Example Policy del bucket con il nome principale del servizio

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
```

```
}
```

Modifica di un prefisso per un bucket esistente

Se cerchi di aggiungere, modificare o rimuovere un prefisso di file di log per un bucket S3 che riceve i log da un percorso, è possibile che venga visualizzato il seguente errore: There is a problem with the bucket policy (Si è verificato un problema con la policy del bucket). Una policy del bucket con un prefisso errato può far sì che un trail non sia in grado di distribuire i log nel bucket. Per risolvere questo problema, usa la console Amazon S3 per aggiornare il prefisso nella policy del bucket, quindi usa la CloudTrail console per specificare lo stesso prefisso per il bucket nel trail.

Per aggiornare il prefisso del file di log per un bucket Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Scegli il bucket per cui modificare il prefisso, quindi Autorizzazioni.
3. Scegli Modifica.
4. Nella policy del bucket, sotto l'`s3:PutObject`azione, modifica la `Resource` voce per aggiungere, modificare o rimuovere il file *`prefix/`* di registro in base alle esigenze.

   ```
   "Action": "s3:PutObject",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*",
   ```

5. Scegli Save (Salva).
6. Apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
7. Scegliere il trail e in Storage location (Percorso di storage) fare clic sull'icona a forma di matita per modificare le impostazioni del bucket.
8. In Bucket S3, scegliere il bucket con il prefisso che si sta modificando.
9. In Log file prefix (Prefisso file di log), aggiornare il prefisso in modo che corrisponda al prefisso immesso nella policy del bucket.
10. Seleziona Salva.

Risorse aggiuntive

Per maggiori informazioni sulle politiche dei bucket S3, consultare Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di Amazon Simple Storage Service.

Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake

Per impostazione predefinita, i bucket e gli oggetti Amazon S3 sono privati. Solo il proprietario della risorsa (l'account AWS che ha creato il bucket) può accedere al bucket e agli oggetti in esso contenuti. Il proprietario della risorsa può concedere le autorizzazioni di accesso ad altre risorse e ad altri utenti mediante una policy di accesso.

Per fornire i risultati delle query CloudTrail Lake a un bucket S3, è CloudTrail necessario disporre delle autorizzazioni richieste e il bucket non può essere configurato come bucket Requester Pays.

CloudTrail aggiunge automaticamente i seguenti campi nella policy:

- I consentiti SIDs
- Nome del bucket
- Il nome principale del servizio per CloudTrail

Come best practice per la sicurezza, aggiungere una chiave di condizione `aws:SourceArn` per la policy del bucket Amazon S3. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire la CloudTrail scrittura nel bucket S3 solo per il data store degli eventi.

La seguente policy consente di inviare i risultati delle query CloudTrail al bucket fornito da Supported. Regioni AWS Sostituisci *`amzn-s3-demo-bucket`* e *`myQueryRunningRegion`* con i valori appropriati per la tua configurazione. *`myAccountID`* *`myAccountID`*È l'ID dell' AWS account utilizzato per CloudTrail, che potrebbe non essere lo stesso dell'ID dell' AWS account per il bucket S3.

> **Note**
>
> Se la policy del bucket include un'istruzione per una chiave KMS, ti consigliamo di utilizzare l'ARN completo della chiave KMS. Se invece utilizzi un alias di chiave KMS, AWS KMS risolve la chiave all'interno dell'account del richiedente. Ciò potrebbe comportare la crittografia dei dati con una chiave KMS di proprietà del richiedente e non del proprietario del bucket.
> Se si tratta di un datastore di eventi dell'organizzazione, l'ARN del datastore di eventi deve includere l'ID account AWS dell'account di gestione, poiché l'account di gestione mantiene la proprietà di tutte le risorse dell'organizzazione.

Policy del bucket S3

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        }
```

```
    ]
}
```

Indice

- Specificare un bucket esistente per i risultati delle query di Lake CloudTrail
- Risorse aggiuntive

Specificare un bucket esistente per i risultati delle query di Lake CloudTrail

Se hai specificato un bucket S3 esistente come posizione di archiviazione per la consegna dei risultati delle query CloudTrail Lake, devi allegare una policy al bucket che consenta di inviare i risultati della query CloudTrail al bucket.

> **Note**
>
> Come best practice, usa un bucket S3 dedicato per i risultati delle query Lake. CloudTrail

Per aggiungere la CloudTrail policy richiesta a un bucket Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Scegli il bucket in cui desideri CloudTrail fornire i risultati delle tue query Lake, quindi scegli Autorizzazioni.
3. Scegliere Edit (Modifica).
4. Copiare la S3 bucket policy for query results nella finestra Bucket Policy Editor (Editor policy bucket). Sostituire i segnaposto in corsivo con i nomi del proprio bucket, la regione e l'ID account.

   > **Note**
   >
   > Se il bucket esistente ha già una o più politiche allegate, aggiungi le istruzioni per l' CloudTrail accesso a quella o alle politiche. Valutare il set di autorizzazioni risultante per assicurarsi che siano appropriate per gli utenti che accedono al bucket.

Risorse aggiuntive

Per maggiori informazioni sulle politiche dei bucket S3, consultare Utilizzo delle policy dei bucket e dell'utente nella Guida per l'utente di Amazon Simple Storage Service.

Policy tematica di Amazon SNS per CloudTrail

Per inviare notifiche a un argomento SNS, è CloudTrail necessario disporre delle autorizzazioni richieste. CloudTrailassegna automaticamente le autorizzazioni richieste all'argomento quando crei un argomento Amazon SNS come parte della creazione o dell'aggiornamento di un percorso nella console. CloudTrail

> **Important**
>
> Come best practice di sicurezza, per limitare l'accesso all'argomento SNS, si consiglia di modificare manualmente la policy IAM allegata all'argomento SNS per aggiungere chiavi della condizione, dopo aver creato o aggiornato un percorso per inviare notifiche SNS. Per ulteriori informazioni, consultare the section called “Best practice di sicurezza per la policy dell'argomento SNS” in questo argomento.

CloudTrail aggiunge automaticamente la seguente dichiarazione alla policy con i seguenti campi:

- I consentiti SIDs.
- Il nome principale del servizio per CloudTrail.
- L'argomento SNS, compresi Regione, ID account e nome argomento.

La seguente politica consente di CloudTrail inviare notifiche sulla consegna dei file di registro dalle regioni supportate. Per ulteriori informazioni, consulta CloudTrail Regioni supportate. Si tratta della policy di default allegata a una policy di argomento SNS nuova o esistente quando crei o aggiorni un percorso e scegli di abilitare le notifiche SNS.

Policy dell'argomento SNS

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:SNSTopicName"
        }
    ]
}
```

Per utilizzare un argomento Amazon SNS AWS KMS crittografato per inviare notifiche, devi anche abilitare la compatibilità tra l'origine dell'evento CloudTrail () e l'argomento crittografato aggiungendo la seguente dichiarazione alla politica di. AWS KMS key

Policy della chiave KMS

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Per ulteriori informazioni, consulta Abilitare la compatibilità tra le fonti di eventi di AWS Services e gli argomenti crittografati.

Indice

- Best practice di sicurezza per la policy dell'argomento SNS
- Specificare un argomento esistente per l'invio di notifiche
- Risoluzione dei problemi della policy dell'argomento SNS
  - CloudTrail non sta inviando notifiche per una regione
  - CloudTrail non sta inviando notifiche per un account membro di un'organizzazione
- Risorse aggiuntive

Best practice di sicurezza per la policy dell'argomento SNS

Per impostazione predefinita, l'informativa sulla policy IAM CloudTrail allegata all'argomento Amazon SNS consente al responsabile CloudTrail del servizio di pubblicare su un argomento SNS, identificato da un ARN. Per impedire a un utente malintenzionato di accedere al tuo argomento SNS e di inviare notifiche per conto dei destinatari dell'argomento, modifica manualmente la policy relativa CloudTrail all'argomento CloudTrail SNS aggiungendo una chiave di `aws:SourceArn` condizione all'informativa sulla policy allegata da. CloudTrail Il valore di questa chiave è l'ARN del percorso o una matrice di percorsi ARNs che utilizzano l'argomento SNS. Poiché include sia l'ID del percorso specifico che l'ID dell'account proprietario del percorso, limita l'accesso all'argomento SNS solo agli account che dispongono dell'autorizzazione per gestire il percorso. Prima di aggiungere le chiavi di condizione alla policy dell'argomento SNS, recupera il nome dell'argomento SNS dalle impostazioni del percorso nella console. CloudTrail

Anche la chiave di condizione `aws:SourceAccount` è supportata, ma non consigliata.

Per aggiungere la chiave della condizione **`aws:SourceArn`** alla policy dell'argomento SNS

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Scegli l'argomento SNS visualizzato nelle impostazioni del percorso, quindi scegli Edit (Modifica).
4. Espandi Access policy (Policy di accesso).
5. Nell'editor JSON Access policy (Policy d'accesso), cerca un blocco simile al seguente esempio.

```
{
```

```
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Aggiungi un nuovo blocco per una condizione, `aws:SourceArn`, come mostrato nell'esempio seguente. Il valore di `aws:SourceArn` è l'ARN del percorso di cui stai inviando notifiche a SNS.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. Al termine della modifica della policy dell'argomento SNS, scegli Save changes (Salva modifiche).

Per aggiungere la chiave della condizione **`aws:SourceAccount`** alla policy dell'argomento SNS

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Scegli l'argomento SNS visualizzato nelle impostazioni del percorso, quindi scegli Edit (Modifica).
4. Espandi Access policy (Policy di accesso).
5. Nell'editor JSON Access policy (Policy d'accesso), cerca un blocco simile al seguente esempio.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Aggiungi un nuovo blocco per una condizione, `aws:SourceAccount`, come mostrato nell'esempio seguente. Il valore di `aws:SourceAccount` è l'ID dell'account proprietario del percorso. CloudTrail Questo esempio limita l'accesso all'argomento SNS solo agli utenti che possono accedere all' AWS account 123456789012.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. Al termine della modifica della policy dell'argomento SNS, scegli Save changes (Salva modifiche).

Specificare un argomento esistente per l'invio di notifiche

Puoi aggiungere manualmente le autorizzazioni per un argomento di Amazon SNS alla tua policy tematica nella console Amazon SNS e quindi specificare l'argomento nella console. CloudTrail

Per aggiornare manualmente una policy di un argomento SNS

1. Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/
2. Scegliere Topics (Argomenti) e quindi l'argomento.
3. Scegli Modifica e scorri verso il basso fino a Politica di accesso.
4. Aggiungi l'estratto conto SNS topic policy con i valori appropriati per la regione, l'ID dell'account e il nome dell'argomento.
5. Se il tuo argomento è crittografato, devi consentire l' CloudTrail accesso `kms:GenerateDataKey*` e le `kms:Decrypt` autorizzazioni. Per ulteriori informazioni, consulta Encrypted SNS topic KMS key policy.
6. Scegli Salva modifiche.
7. Tornate alla CloudTrail console e specificate l'argomento del percorso.

Risoluzione dei problemi della policy dell'argomento SNS

Le seguenti sezioni descrivono come risolvere i problemi relativi alla policy degli argomenti SNS.

Scenari:

- CloudTrail non sta inviando notifiche per una regione
- CloudTrail non sta inviando notifiche per un account membro di un'organizzazione

CloudTrail non sta inviando notifiche per una regione

Quando crei un nuovo argomento come parte della creazione o dell'aggiornamento di un percorso, CloudTrail assegna le autorizzazioni necessarie all'argomento. La politica dell'argomento utilizza il nome principale del servizio`"cloudtrail.amazonaws.com"`, che consente di CloudTrail inviare notifiche per tutte le regioni.

Se non invia notifiche per una regione, CloudTrail è possibile che l'argomento abbia una politica precedente che specifica l' CloudTrail account IDs per ciascuna regione. Questo tipo di politica CloudTrail autorizza l'invio di notifiche solo per le regioni specificate.

Come procedura ottimale, aggiorna la politica per utilizzare un'autorizzazione con il responsabile del CloudTrail servizio. A tale scopo, sostituisci l'ID dell'account ARNs con il nome principale del servizio:`"cloudtrail.amazonaws.com"`.

La seguente politica di esempio CloudTrail consente di inviare notifiche per le regioni attuali e nuove:

Example Policy dell'argomento con il nome principale del servizio

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

Verifica che la policy includa i valori corretti:

- Nel campo `Resource`, specificare il numero di account del proprietario dell'argomento. Per gli argomenti creati specificare il numero di account.
- Specifica i valori appropriati per la Regione e il nome dell'argomento SNS.

CloudTrail non sta inviando notifiche per un account membro di un'organizzazione

Quando un account membro con un percorso AWS Organizations organizzativo non invia notifiche Amazon SNS, potrebbe esserci un problema con la configurazione della policy tematica SNS. CloudTrail crea percorsi organizzativi negli account dei membri anche se la convalida di una risorsa fallisce, ad esempio, l'argomento SNS dell'organization trail non include tutti gli account dei membri. IDs Se la policy dell'argomento SNS non è corretta, si verifica un errore di autorizzazione.

Per verificare se la policy degli argomenti SNS di un percorso presenta un errore di autorizzazione:

- Dalla CloudTrail console, controlla la pagina dei dettagli del percorso. Se si verifica un errore di autorizzazione, la pagina dei dettagli include un avviso `SNS authorization failed` e indica di correggere la politica dell'argomento SNS.
- Da AWS CLI, esegui il get-trail-statuscomando. Se si verifica un errore di autorizzazione, l'output del comando include il `LastNotificationError` campo con un valore di`AuthorizationError`.

Risorse aggiuntive

Per informazioni sugli argomenti Amazon SNS e sulla relativa sottoscrizione, consulta la Guida per sviluppatori di Amazon Simple Notification Service.

Risoluzione dei problemi relativi AWS CloudTrail all'identità e all'accesso

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

Argomenti

- Non sono autorizzato a eseguire alcuna azione in CloudTrail
- Non sono autorizzato a eseguire iam:PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie CloudTrail risorse
- Non sono autorizzato a eseguire iam:PassRole
- Ricevo un'eccezione NoManagementAccountSLRExistsException quando provo a creare un percorso dell'organizzazione o un datastore di eventi

Non sono autorizzato a eseguire alcuna azione in CloudTrail

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `cloudtrail:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `cloudtrail:`*`GetWidget`*.

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

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli di un percorso ma non dispone della politica CloudTrail gestita appropriata (AWSCloudTrail_FullAccesso AWSCloudTrail_ReadOnlyAccess) o delle autorizzazioni equivalenti applicate al suo account.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy che gli consentono di accedere alle informazioni sul trail e allo stato nella console.

Se accedi con un utente o un ruolo IAM con la policy AWSCloudTrail_FullAccessgestita o le relative autorizzazioni equivalenti e non riesci a configurare AWS Config l'integrazione di Amazon CloudWatch Logs con un trail, potresti non avere le autorizzazioni necessarie per l'integrazione con tali servizi. Per ulteriori informazioni, consultare Concessione dell'autorizzazione alla visualizzazione delle AWS Config informazioni sulla console CloudTrail e Concessione dell'autorizzazione a visualizzare e configurare le informazioni di Amazon CloudWatch Logs sulla console CloudTrail .

Non sono autorizzato a eseguire **`iam:PassRole`**

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a CloudTrail.

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

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

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

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

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

Voglio consentire a persone esterne a me di accedere Account AWS alle mie CloudTrail risorse

Puoi creare un ruolo e condividere CloudTrail informazioni tra più persone Account AWS. Per ulteriori informazioni, consulta Condivisione di file di CloudTrail registro tra AWS account.

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

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se CloudTrail supporta queste funzionalità, consulta. Come AWS CloudTrail funziona con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Non sono autorizzato a eseguire **`iam:PassRole`**

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a CloudTrail.

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

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

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

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

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

Ricevo un'eccezione **`NoManagementAccountSLRExistsException`** quando provo a creare un percorso dell'organizzazione o un datastore di eventi

L'eccezione `NoManagementAccountSLRExistsException` viene generata quando l'account di gestione non ha un ruolo collegato al servizio.

Quando aggiungi un amministratore delegato utilizzando l'operazione AWS Organizations CLI o API CloudTrail , i ruoli collegati ai servizi non verranno creati automaticamente se non esistono. I ruoli collegati al servizio vengono creati solo quando si effettua una chiamata dall'account di gestione direttamente al servizio. CloudTrail Ad esempio, quando si aggiunge un amministratore delegato o si crea un percorso organizzativo o un data store di eventi utilizzando la CloudTrail console AWS CLI o l' CloudTrail API, viene creato il ruolo collegato al AWSServiceRoleForCloudTrail servizio.

Quando aggiungi un amministratore delegato utilizzando l'operazione AWS CloudTrail; CLI o API CloudTrail , creerà sia AWSServiceRoleForCloudTrail il ruolo che il ruolo collegato al servizio. AWSServiceRoleForCloudTrailEventContext

Quando si utilizza l'account di gestione dell'organizzazione per aggiungere un amministratore delegato o creare un organigramma o un data store di eventi nella CloudTrail console, oppure utilizzando l' CloudTrailAPI AWS CLI o, crea CloudTrail automaticamente il ruolo AWSServiceRoleForCloudTrail collegato ai servizi per l'account di gestione, se questo non esiste già. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per CloudTrail.

Se non hai aggiunto un amministratore delegato, utilizza la CloudTrail console AWS CLI o l' CloudTrail API per aggiungere l'amministratore delegato. Per ulteriori informazioni sull'aggiunta di un amministratore delegato, consulta Aggiunta di un CloudTrail amministratore delegato and RegisterOrganizationDelegatedAdmin(API).

Se hai già aggiunto l'amministratore delegato, utilizza l'account di gestione per creare l'organigramma o il data store degli eventi nella CloudTrail console oppure utilizzando l'API AWS CLI o CloudTrail . Per ulteriori informazioni sulla creazione di un percorso organizzativo, consulta Creazione di un percorso per la tua organizzazione nella consoleCreare un percorso per un'organizzazione con AWS CLI, and CreateTrail(API).

Utilizzo di ruoli collegati ai servizi per CloudTrail

AWS CloudTrail utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. CloudTrail I ruoli collegati ai servizi sono predefiniti CloudTrail e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Argomenti

- Utilizzo dei ruoli per la creazione e la gestione dei percorsi CloudTrail organizzativi e degli archivi dati degli eventi di CloudTrail Lake Organization in CloudTrail
- Regioni supportate per i ruoli collegati ai servizi CloudTrail
- Utilizzo dei ruoli per la creazione e la gestione del contesto degli CloudTrail eventi in CloudTrail
- Regioni supportate per i ruoli collegati ai servizi CloudTrail

Utilizzo dei ruoli per la creazione e la gestione dei percorsi CloudTrail organizzativi e degli archivi dati degli eventi di CloudTrail Lake Organization in CloudTrail

AWS CloudTrail utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. CloudTrail I ruoli collegati ai servizi sono predefiniti CloudTrail e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione CloudTrail perché non è necessario aggiungere manualmente le autorizzazioni necessarie. CloudTrail definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. CloudTrail Le

autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi CloudTrail le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per CloudTrail

CloudTrail utilizza il ruolo collegato al servizio denominato AWSServiceRoleForCloudTrail: questo ruolo collegato al servizio viene utilizzato per supportare gli itinerari organizzativi e gli archivi dati degli eventi organizzativi.

Il ruolo AWSService RoleForCloudTrail collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `cloudtrail.amazonaws.com`

La politica di autorizzazione dei ruoli denominata CloudTrailServiceRolePolicy consente di CloudTrail completare le seguenti azioni sulle risorse specificate:

- Azioni su tutte le CloudTrail risorse:
  - `All`
- Azioni su tutte le AWS Organizations risorse:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Azioni su tutte le risorse di Organizations per il responsabile del CloudTrail servizio per elencare gli amministratori delegati dell'organizzazione:
  - `organizations:ListDelegatedAdministrators`
- Operazioni per disabilitare la federazione di Data Lake in un datastore di eventi dell'organizzazione:

- `glue:DeleteTable`
- `lakeformation:DeRegisterResource`

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Per ulteriori informazioni sulla politica gestita associata a AWSServiceRoleForCloudTrail, vedere. AWS politiche gestite per AWS CloudTrail

Creazione di un ruolo collegato ai servizi per CloudTrail

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un organigramma o un data store per eventi organizzativi o aggiungi un amministratore delegato nella CloudTrail console AWS Management Console, nell'API o nell' AWS CLI AWS API, CloudTrail crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un organigramma o un data store per eventi organizzativi o aggiungi un amministratore delegato nella CloudTrail console, CloudTrail crea nuovamente il ruolo collegato ai servizi.

Modifica di un ruolo collegato ai servizi per CloudTrail

CloudTrail non consente di modificare il ruolo collegato al AWSService RoleForCloudTrail servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per CloudTrail

Non è necessario eliminare manualmente il AWSService RoleForCloudTrail ruolo. Se un Account AWS viene rimosso da un'organizzazione Organizations, il AWSServiceRoleForCloudTrail ruolo viene rimosso automaticamente da tale organizzazione Account AWS. Non puoi distaccare o rimuovere policy dal ruolo collegato al servizio AWSServiceRoleForCloudTrail in un account di gestione dell'organizzazione senza rimuovere l'account dall'organizzazione.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, devi prima effettuare manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi è possibile eliminarlo manualmente.

> **Note**
>
> Se il CloudTrail servizio utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per rimuovere una risorsa utilizzata da quel ruolo AWSServiceRoleForCloudTrail, è possibile eseguire una delle operazioni seguenti:

- Rimuovi il Account AWS dall'organizzazione in Organizations.
- Aggiornare il trail che non è più il trail di un'organizzazione. Per ulteriori informazioni, consulta Aggiornamento di un percorso con la CloudTrail console.
- Aggiorna il datastore di eventi in modo che non sia più un datastore di eventi dell'organizzazione. Per ulteriori informazioni, consulta Aggiorna un data store di eventi con la console.
- Eliminare il trail. Per ulteriori informazioni, consulta Eliminazione di un percorso con la console CloudTrail .
- Elimina il datastore di eventi. Per ulteriori informazioni, consulta Eliminare un archivio dati di eventi con la console.

Eliminazione manuale del ruolo collegato al servizio con IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo AWSServiceRoleForCloudTrail collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi CloudTrail

CloudTrail supporta l'utilizzo di ruoli collegati ai servizi in tutte le aree in Regioni AWS cui sono disponibili sia CloudTrail Organizations che Organizations. Per ulteriori informazioni, consulta la sezione relativa a regioni ed endpoint AWS nella Riferimenti generali di AWS.

Utilizzo dei ruoli per la creazione e la gestione del contesto degli CloudTrail eventi in CloudTrail

AWS CloudTrail utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. CloudTrail I ruoli

collegati ai servizi sono predefiniti CloudTrail e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione CloudTrail perché non è necessario aggiungere manualmente le autorizzazioni necessarie. CloudTrail definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. CloudTrail Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi CloudTrail le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per CloudTrail

CloudTrail utilizza il ruolo collegato al servizio denominato AWSServiceRoleForCloudTrailEventContext: questo ruolo collegato al servizio viene utilizzato per gestire CloudTrail il contesto e le regole dell'evento. EventBridge

Il ruolo AWSService RoleForCloudTrailEventContext collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `context.cloudtrail.amazonaws.com`

La politica di autorizzazione dei ruoli denominata CloudTrailEventContext consente di CloudTrail completare le seguenti azioni sulle risorse specificate:

- Azioni sui tag delle risorse:
  - `tag:GetResources`
- Azioni su tutte le EventBridge risorse Amazon affinché il responsabile del CloudTrail servizio crei regole:
  - `events:PutRule`
- Azioni su tutte le EventBridge risorse Amazon per consentire al responsabile del CloudTrail servizio di gestire le regole che crea:

  - `events:PutTargets`
  - `events:DeleteRule`
  - `events:RemoveTargets`
  - `events:RemoveTargets`
- Azioni su tutte le EventBridge risorse Amazon per il responsabile del CloudTrail servizio per descrivere le regole che crea:
  - `events:DescribeRule`
  - `events:DeRegisterResource`
- Azioni su tutte le EventBridge risorse Amazon:
  - `events:ListRules`

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Per ulteriori informazioni sulla politica gestita associata a AWSServiceRoleForCloudTrailEventContext, consultaAWS politiche gestite per AWS CloudTrail.

Creazione di un ruolo collegato ai servizi per CloudTrail

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando inizi a utilizzare la funzionalità relativa agli eventi contestuali nell' AWS Management Console AWS CLI, nella o nell' AWS API, CloudTrail crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando inizi a utilizzare la funzionalità degli eventi contestuali, CloudTrail crea nuovamente il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per CloudTrail

CloudTrail non consente di modificare il ruolo collegato al AWSService RoleForCloudTrailEventContext servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al servizio per AWSService RoleForCloudTrailEventContext CloudTrail

Se non è più necessario utilizzare una funzionalità o un servizio che richiede il ruolo AWSService RoleForCloudTrailEventContext collegato al servizio, si consiglia di eliminare tale ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario ripulire le risorse per il ruolo collegato al servizio prima di poterlo eliminare manualmente rimuovendo la TagContext chiave dagli archivi dati degli eventi.

> **Note**
>
> Se il CloudTrail servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare CloudTrail le risorse utilizzate dal ruolo collegato al AWSService RoleForCloudTrailEventContext servizio

1. Nel terminale o nella riga di comando, esegui il put-event-configuration comando per l'archivio eventi da cui desideri rimuovere la `TagContext` chiave. Ad esempio, per rimuovere la `TagContext` chiave da un archivio eventi nell'*111122223333*account nella regione Stati Uniti orientali (Ohio) con un ARN *`arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`* di `TagContext` where è l'unico selettore di chiavi di contesto, è necessario utilizzare put-event-configuration il comando senza specificare alcun valore per: `--context-key-selectors`

   ```
   aws cloudtrail put-event-configuration --event-data-store arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --max-event-size Large --context-key-selectors
   ```

2. Ripeti questo comando per ogni archivio dati in ogni regione della partizione. Per ulteriori informazioni, consulta Identificare AWS le risorse con Amazon Resource Names (ARNs).

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSService RoleForCloudTrailEventContext collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi CloudTrail

CloudTrail supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui CloudTrail e sono disponibili. EventBridge Per ulteriori informazioni, consulta AWS Regioni ed endpoint.

AWS politiche gestite per AWS CloudTrail

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le policy AWS gestite che scriverle autonomamente. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le policy AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: **`AWSCloudTrail_FullAccess`**

Un'identità utente a cui è associata la AWSCloudTrail_FullAccesspolitica associata al proprio ruolo ha accesso amministrativo completo CloudTrail.

Per un elenco in JSON dei dettagli della policy, consulta la guida AWSCloudTrail_FullAccessdi riferimento della politica AWS gestita.

AWS politica gestita: **`AWSCloudTrail_ReadOnlyAccess`**

Un'identità utente a cui è associata la AWSCloudTrail_ReadOnlyAccesspolicy al proprio ruolo può eseguire azioni di sola lettura in CloudTrail, ad esempio `Get*List*`, `Describe*` azioni su trail, archivi dati di eventi CloudTrail Lake o query Lake.

Per un elenco in JSON dei dettagli della policy, consulta AWSCloudTrail_ReadOnlyAccessla guida di riferimento AWS Managed Policy.

AWS politica gestita: **`AWSServiceRoleForCloudTrail`**

La CloudTrailServiceRolePolicypolicy consente di AWS CloudTrail eseguire azioni sui percorsi organizzativi e sugli archivi di dati degli eventi organizzativi per conto dell'utente. La politica include AWS Organizations le autorizzazioni necessarie per descrivere ed elencare gli account dell'organizzazione e gli amministratori delegati di un'organizzazione. AWS Organizations

Questa politica include inoltre le autorizzazioni necessarie AWS Glue e le AWS Lake Formation autorizzazioni per disabilitare Lake Federation su un data store di eventi dell'organizzazione.

Questa policy è associata al ruolo AWSServiceRoleForCloudTrailcollegato al servizio che consente di eseguire azioni CloudTrail per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Per un elenco in JSON dei dettagli della policy, consulta CloudTrailServiceRolePolicyla guida di riferimento della politica AWS gestita.

AWS politica gestita: **`CloudTrailEventContext`**

La CloudTrailEventContextpolitica consente di AWS CloudTrail gestire il contesto e EventBridge le regole CloudTrail dell'evento per tuo conto. La politica include EventBridge le autorizzazioni necessarie per creare, gestire e descrivere le regole che crea per te.

Questa politica è associata al ruolo AWSServiceRoleForCloudTrailEventContextcollegato al servizio che consente di eseguire azioni CloudTrail per conto dell'utente. Non puoi collegare questa policy ai tuoi utenti, gruppi o ruoli.

Per un elenco in JSON dei dettagli della policy, consulta CloudTrailEventContextla guida di riferimento della politica AWS gestita.

CloudTrail aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per CloudTrail. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina CloudTrail Cronologia dei documenti.

Modifica	Descrizione	Data
`CloudTrailEventContext` — Nuova politica utilizzata dal ruolo collegato al `AWSServiceRoleForCloudTrailEventContext` servizio	Aggiunti una nuova politica e un nuovo ruolo utilizzati per la funzionalità di eventi CloudTrail arricchita.	19 maggio 2025
`CloudTrailServiceRolePolicy`: aggiornamento a una policy esistente	La policy è stata aggiornata per consentire le seguenti operazioni in un datastore di eventi dell'organizzazione e quando la federazione è disabilitata: • `glue:DeleteTable` • `lakeformation:DeregisterResource`	26 novembre 2023
`AWSCloudTrail_ReadOnlyAccess`: aggiornamento a una policy esistente	CloudTrail ha cambiato il nome della `AWSCloudTrailReadOnlyAccess` politica in. `AWSCloudTrail_ReadOnlyAccess` Inoltre, l'ambito delle autorizzazioni nella politica è stato ridotto alle CloudTrail azioni. Non include più Amazon S3 o le autorizzazioni AWS KMS di AWS Lambda azione.	6 giugno 2022

Modifica	Descrizione	Data
CloudTrail ha iniziato a tenere traccia delle modifiche	CloudTrail ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	6 giugno 2022

Convalida della conformità per AWS CloudTrail

I revisori di terze parti valutano la sicurezza e la conformità nell' AWS CloudTrail ambito di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

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

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

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS CloudTrail

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. Se hai specificamente bisogno di replicare i tuoi file di CloudTrail log su distanze geografiche maggiori, puoi utilizzare la replica interregionale per i tuoi bucket trail Amazon S3, che consente la copia automatica e asincrona di oggetti tra bucket in diverse regioni. AWS

Per ulteriori informazioni su regioni e zone di disponibilità, consulta Global Infrastructure. AWSAWS

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

Percorsi e archivi di dati sugli eventi che registrano gli eventi in tutte le regioni AWS

Quando crei un percorso multiregionale, CloudTrail crea percorsi con configurazioni identiche, tutte abilitate Regioni AWS nel tuo account.

Quando crei un archivio dati di eventi multiregionale, CloudTrail raccoglie tutti Regioni AWS gli eventi che si verificano nel tuo account.

Controllo delle versioni, configurazione del ciclo di vita e protezione del blocco oggetti per i dati di registrazione di CloudTrail

Poiché CloudTrail utilizza i bucket Amazon S3 per archiviare i file di registro, puoi anche utilizzare le funzionalità fornite da Amazon S3 per supportare le tue esigenze di resilienza e backup dei dati. Per maggiori informazioni, consulta Resilienza in Amazon S3.

Sicurezza dell'infrastruttura in AWS CloudTrail

In quanto servizio gestito, AWS CloudTrail è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di 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.

Utilizzate chiamate API AWS pubblicate per accedere CloudTrail 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.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Le seguenti best practice di sicurezza riguardano anche la sicurezza dell'infrastruttura in CloudTrail:

- Considerare gli endpoint Amazon VPC l'accesso al trail.
- Considera gli endpoint Amazon VPC per l'accesso ai bucket Amazon S3. Per ulteriori informazioni, consulta Controllo dell'accesso dagli endpoint VPC con policy bucket.
- Identifica e controlla tutti i bucket Amazon S3 che contengono CloudTrail file di log. Prendi in considerazione l'utilizzo di tag per identificare sia i CloudTrail percorsi che i bucket Amazon S3 che contengono CloudTrail i file di registro. Puoi quindi utilizzare i gruppi di risorse per le tue CloudTrail risorse. Per ulteriori informazioni, consulta AWS Resource Groups.

Prevenzione del problema "confused deputy" tra servizi

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

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che AWS CloudTrail forniscono un altro servizio alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Quando si include un carattere jolly, è necessario utilizzare l'operatore condizionale `StringLike`.

Il valore di `aws:SourceArn` deve essere l'ARN del percorso, del datastore di eventi o del canale che utilizza la risorsa.

L'esempio seguente mostra come è possibile utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition CloudTrail per evitare il confuso problema del vice:Policy sui bucket di Amazon S3 per CloudTrail i risultati delle query Lake.

Le migliori pratiche di sicurezza in AWS CloudTrail

AWS CloudTrail fornisce una serie di funzionalità di sicurezza da considerare 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.

Argomenti

- CloudTrail best practice in materia di sicurezza investigativa
- CloudTrail best practice di sicurezza preventiva

CloudTrail best practice in materia di sicurezza investigativa

Creazione di un trail

Per una registrazione continua degli eventi nel tuo AWS account, devi creare un percorso. Sebbene CloudTrail fornisca 90 giorni di informazioni sulla cronologia degli eventi per gli eventi di gestione nella CloudTrail console senza creare un percorso, non è un record permanente e non fornisce informazioni su tutti i possibili tipi di eventi. Per un record in corso e per un record che contiene tutti i tipi di eventi specificati devi creare un percorso che fornisca i relativi file di log per un bucket Amazon S3 specificato.

Per facilitare la gestione CloudTrail dei dati, prendi in considerazione la creazione di un percorso che registri tutti Regioni AWS gli eventi di gestione e quindi la creazione di percorsi aggiuntivi che registrino tipi di eventi specifici per le risorse, come l'attività o le funzioni dei bucket di Amazon S3. AWS Lambda

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Creazione di un trail per l'account AWS .
- Creazione di un trail per un'organizzazione.

Crea un percorso multiregionale

Per ottenere un record completo degli eventi registrati da un'identità o da un servizio IAM nel tuo AWS account, crea un percorso multiregionale. I percorsi multiregionali registrano gli eventi in tutto ciò Regioni AWS che è abilitato nel tuo. Account AWS Registrando gli eventi in tutte le aree abilitate Regioni AWS, vi assicurate di registrare l'attività in tutte le regioni abilitate del vostro. Account AWS Ciò include la registrazione degli eventi di servizio globali, che vengono registrati su uno Regione AWS specifico servizio. Tutti i percorsi creati utilizzando la CloudTrail console sono percorsi multiregionali.

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Creazione di un trail per l'account AWS .
- Converti un itinerario esistente a regione singola in un percorso multiregionale.
- Implementa controlli investigativi continui per garantire che tutti i percorsi creati registrino tutti gli eventi Regioni AWS utilizzando la regola multi-region-cloud-trail-enabled in. AWS Config

Abilita l'integrità dei file di CloudTrail registro

I file di log convalidati sono particolarmente preziosi nelle indagini giudiziarie e sulla sicurezza. Ad esempio, un file di log convalidato consente di confermare senza ombra di dubbio che tale file non ha subito modifiche oppure che una specifica attività API è stata eseguita utilizzando credenziali di un'identità IAM attendibile. Il processo di convalida dell'integrità dei file di CloudTrail registro consente inoltre di sapere se un file di registro è stato eliminato o modificato o di affermare con certezza che nessun file di registro è stato inviato all'account durante un determinato periodo di tempo. CloudTrail la convalida dell'integrità dei file di registro utilizza algoritmi standard del settore: SHA-256 per l'hashing e SHA-256 con RSA per la firma digitale. Ciò rende computazionalmente impossibile modificare, eliminare o falsificare i file di registro senza essere rilevati. CloudTrail Per ulteriori informazioni, consulta Abilitazione della convalida e convalida dei file.

Integrazione con Amazon CloudWatch Logs

CloudWatch Logs ti consente di monitorare e ricevere avvisi per eventi specifici acquisiti da. CloudTrail Gli eventi inviati a CloudWatch Logs sono quelli configurati per essere registrati dal tuo percorso, quindi assicurati di aver configurato il percorso o i percorsi per registrare i tipi di eventi (eventi di gestione, eventi relativi ai dati e/o eventi di attività di rete) che desideri monitorare.

Ad esempio, puoi monitorare gli eventi chiave relativi alla sicurezza e alla gestione della rete, come gli eventi di accesso non riuscito. AWS Management Console

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Consulta l'esempio CloudWatch di integrazioni di Logs per. CloudTrail
- Configura il tuo percorso per inviare eventi ai registri. CloudWatch
- Prendi in considerazione l'implementazione di controlli investigativi continui per garantire che tutti i trail inviino eventi a CloudWatch Logs per il monitoraggio utilizzando la regola cloud-trail-cloud-watch-logs-enabled in. AWS Config

Usa Amazon GuardDuty

Amazon GuardDuty è un servizio di rilevamento delle minacce che ti aiuta a proteggere account, container, carichi di lavoro e dati all'interno del tuo AWS ambiente. Utilizzando modelli di machine learning (ML) e funzionalità di rilevamento di anomalie e minacce, monitora GuardDuty continuamente diverse fonti di log per identificare e dare priorità ai potenziali rischi per la sicurezza e alle attività dannose nel tuo ambiente.

Ad esempio, GuardDuty rileverà la potenziale esfiltrazione di credenziali nel caso in cui rilevi credenziali create esclusivamente per un' EC2 istanza Amazon tramite un ruolo di avvio dell'istanza ma utilizzate da un altro account all'interno. AWS Per ulteriori informazioni, consulta la Amazon GuardDuty User Guide.

Utilizza AWS Security Hub

Monitora il tuo utilizzo CloudTrail in relazione alle migliori pratiche di sicurezza utilizzando AWS Security Hub. Centrale di sicurezza utilizza controlli di sicurezza di investigazione per valutare le configurazioni delle risorse e gli standard di sicurezza per aiutarti a rispettare vari framework di conformità. Per ulteriori informazioni sull'utilizzo di Security Hub per valutare CloudTrail le risorse, vedere AWS CloudTrail i controlli nella Guida AWS Security Hub per l'utente.

CloudTrail best practice di sicurezza preventiva

Le seguenti best practice CloudTrail possono aiutare a prevenire incidenti di sicurezza.

Registrazione in un bucket Amazon S3 dedicato e centralizzato

CloudTrail i file di registro sono un registro di controllo delle azioni intraprese da un'identità o da un AWS servizio IAM. L'integrità, la completezza e la disponibilità di questi log è cruciale per scopi forensi e di auditing. Effettuando la registrazione in un bucket Amazon S3 dedicato e centralizzato, puoi applicare rigorosi controlli di sicurezza, accesso e separazione dei compiti.

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Crea un AWS account separato come account di archivio dei registri. Se lo utilizzi AWS Organizations, registra questo account nell'organizzazione e valuta la possibilità di creare un percorso organizzativo per registrare i dati di tutti gli AWS account dell'organizzazione.
- Se non utilizzi Organizations ma desideri registrare i dati per più AWS account, crea un percorso per registrare le attività in questo account di archivio dei registri. Limitare l'accesso a questo

account ai soli utenti amministrativi affidabili che devono avere accesso ai dati di auditing e dell'account.

- Come parte della creazione di un percorso, che si tratti di un percorso dell'organizzazione o di un percorso per un singolo AWS account, crea un bucket Amazon S3 dedicato per archiviare i file di registro per questo percorso.
- Se desideri registrare l'attività per più di un AWS account, modifica la policy del bucket per consentire la registrazione e l'archiviazione dei file di registro per tutti gli AWS account su cui desideri registrare l'attività dell'account. AWS
- Se non utilizzi un percorso dell'organizzazione, crea percorsi in tutti gli account AWS , specificando il bucket Amazon S3 nell'account archivio di log.

Utilizza la crittografia lato server con chiavi gestite AWS KMS

Per impostazione predefinita, i file di registro forniti dal CloudTrail bucket S3 sono crittografati utilizzando la crittografia lato server con una chiave KMS (SSE-KMS). Per utilizzare SSE-KMS con CloudTrail, devi creare e gestire una, nota anche come chiave KMS. AWS KMS key

> **Note**
>
> Se utilizzi SSE-KMS e la convalida dei file di registro e hai modificato la tua policy sui bucket di Amazon S3 per consentire solo i file crittografati SSE-KMS, non sarai in grado di creare percorsi che utilizzino quel bucket a meno che non modifichi la policy del bucket per consentire specificamente la crittografia, come mostrato nella seguente riga di policy di esempio. AES256
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Esaminare i vantaggi della crittografia dei file di log con SSE-KMS.
- Crea una chiave KMS da utilizzare per la crittografia dei file di log.
- Configurare la crittografia del file di log per i trail.
- Prendi in considerazione l'implementazione di controlli investigativi continui per garantire che tutti i trail crittografino i file di registro con SSE-KMS utilizzando la cloud-trail-encryption-enabledregola in AWS Config.

Aggiunta di una chiave di condizione alla policy predefinita dell'argomento Amazon SNS

Quando configuri un trail per inviare notifiche ad Amazon SNS, CloudTrail aggiunge una dichiarazione di policy alla policy di accesso agli argomenti SNS che consente di inviare contenuti CloudTrail a un argomento SNS. Come best practice di sicurezza, consigliamo di aggiungere una chiave di condizione `aws:SourceArn` (o facoltativamente`aws:SourceAccount`) alla dichiarazione sulla policy tematica di Amazon SNS. Ciò consente di impedire l'accesso non autorizzato all'account all'argomento SNS. Per ulteriori informazioni, consulta Policy tematica di Amazon SNS per CloudTrail.

Implementazione dell'accesso con privilegio minimo ai bucket Amazon S3 in cui si archiviano i file di log

CloudTrail traccia gli eventi in un bucket Amazon S3 specificato dall'utente. Questi file di registro contengono un registro di controllo delle azioni intraprese dalle identità e dai servizi IAM. AWS L'integrità e la completezza di questi file di log sono fondamentali a scopo forense e di auditing. Per contribuire a garantire tale integrità, è necessario rispettare il principio del privilegio minimo quando si crea o si modifica l'accesso a qualsiasi bucket Amazon S3 utilizzato per archiviare i file di registro. CloudTrail

Utilizza le fasi seguenti:

- Esaminare le policy dei bucket di Amazon S3 per tutti i bucket in cui si archiviano i file di log e adattarla, se necessario, per rimuovere qualsiasi accesso inutile. Questa policy sui bucket verrà generata automaticamente se crei un trail utilizzando la CloudTrail console, ma può anche essere creata e gestita manualmente.
- Come best practice per la sicurezza, assicurati di aggiungere manualmente una chiave di condizione `aws:SourceArn` per la policy del bucket. Per ulteriori informazioni, consulta Policy sui bucket Amazon S3 per CloudTrail.
- Se stai usando lo stesso bucket Amazon S3 per archiviare i file di log per più account AWS , segui le indicazioni per la ricezione di file di log per più account.
- Se stai utilizzando un percorso dell'organizzazione, verifica di seguire le indicazioni per i percorsi dell'organizzazione ed esamina le policy di esempio per un bucket Amazon S3 per un percorso dell'organizzazione in Creare un percorso per un'organizzazione con AWS CLI.
- Consulta la documentazione della sicurezza di Amazon S3 e la spiegazione passo per passo di esempio per proteggere un bucket.

Abilitazione dell'eliminazione MFA sul bucket Amazon S3 in cui si archiviano i file di log

La configurazione dell'autenticazione a più fattori (MFA) garantisce che qualsiasi tentativo di modificare lo stato di controllo delle versioni del bucket oppure di eliminare in modo permanente una versione di un oggetto richiede un ulteriore livello di autenticazione. In questo modo, anche se un utente acquisisse una password di un utente IAM con autorizzazioni per eliminare definitivamente gli oggetti Amazon S3, sarà comunque possibile impedire operazioni che potrebbero compromettere i file di log.

Di seguito sono riportate alcune delle procedure che è possibile eseguire:

- Consulta la procedura di eliminazione tramite MFA nella Guida per l'utente di Amazon Simple Storage Service.
- Aggiungi una policy del bucket Amazon S3 per richiedere l'autenticazione MFA.

> **Note**
>
> Non puoi utilizzare l'eliminazione MFA con le configurazioni del ciclo di vita. Per ulteriori informazioni sulle configurazioni del ciclo di vita e sul modo in cui interagiscono con altre configurazioni, consulta Configurazioni del ciclo di vita e altre configurazioni del bucket nella Guida per l'utente di Amazon Simple Storage Service.

Configurazione della gestione del ciclo di vita dell'oggetto nel bucket Amazon S3 in cui si archiviano i file di log

L'impostazione predefinita del CloudTrail percorso consiste nell'archiviare i file di registro a tempo indeterminato nel bucket Amazon S3 configurato per il percorso. È possibile utilizzare le regole d gestione del ciclo di vita di oggetti di Amazon S3 per definire le policy di conservazione per soddisfare al meglio le esigenze dell'azienda e le esigenze di auditing. Ad esempio, è possibile archiviare i file di log creati da più di un anno in Amazon Glacier o eliminare i file di log dopo un determinato periodo di tempo.

> **Note**
>
> La configurazione del ciclo di vita su bucket abilitati a più fattori (MFA) non è supportata.

Limita l'accesso alla policy AWSCloudTrail_FullAccess

Gli utenti che dispongono della AWSCloudTrail_FullAccesspolicy hanno la possibilità di disabilitare o riconfigurare le funzioni di controllo più sensibili e importanti nei propri AWS account. Questa policy non è progettata per essere condivisa o applicata globalmente alle identità IAM nell'account AWS . Limita l'applicazione di questa politica al minor numero possibile di persone, quelle che ti aspetti che agiscano come amministratori di AWS account.

Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS)

Per impostazione predefinita, i file di registro e i file digest forniti dal CloudTrail bucket vengono crittografati utilizzando la crittografia lato server con una chiave KMS (SSE-KMS). Se non abiliti la crittografia SSE-KMS, i file di log e i file digest vengono crittografati utilizzando la crittografia SSE-S3.

> **Note**
>
> Se stai utilizzando un bucket S3 esistente con una chiave del bucket S3, CloudTrail devi disporre dell'autorizzazione nella policy chiave per utilizzare le azioni e. AWS KMS `GenerateDataKey` `DescribeKey` Se a `cloudtrail.amazonaws.com` non sono concesse tali autorizzazioni nella policy della chiave, non puoi creare o aggiornare un percorso.

Per utilizzare SSE-KMS con CloudTrail, crei e gestisci un. AWS KMS key Si allega una politica alla chiave che determina quali utenti possono utilizzare la chiave per crittografare e decrittografare CloudTrail i file di registro e i file digest. La decrittografia è un processo seamless in S3. Quando gli utenti autorizzati della chiave leggono i file di CloudTrail registro o i file digest, S3 gestisce la decrittografia e gli utenti autorizzati sono in grado di leggere i file in formato non crittografato.

Questo approccio presenta i vantaggi seguenti:

- Puoi creare e gestire tu stesso la chiave KMS.
- Puoi utilizzare una singola chiave KMS per crittografare e decrittografare i file di registro e i file digest per più account in tutte le regioni.
- Hai il controllo su chi può utilizzare la tua chiave per crittografare e CloudTrail decrittografare i file di registro e i file digest. Puoi assegnare le autorizzazioni per la chiave agli utenti nell'organizzazione in base alle tue esigenze.

- Disponi di una sicurezza avanzata. Con questa funzionalità, per leggere i file di registro o i file digest, sono necessarie le seguenti autorizzazioni:
  - Un utente deve disporre delle autorizzazioni di lettura S3 per il bucket che contiene i file di log e i file digest.
  - Un utente deve disporre di una policy o di un ruolo che consente di decrittare le autorizzazioni applicate dalla policy della chiave KMS.
- Poiché S3 decrittografa automaticamente i file di registro e i file digest per le richieste degli utenti autorizzati a utilizzare la chiave KMS, la crittografia SSE-KMS per i file è retrocompatibile con le applicazioni che leggono i dati di registro. CloudTrail

> **Note**
>
> La chiave KMS scelta deve essere creata nella stessa AWS regione del bucket Amazon S3 che riceve i file di log e i file digest. Ad esempio, se i file di log e i file digest verranno archiviati in un bucket nella regione Stati Uniti orientali (Ohio), devi creare o scegliere una chiave KMS creata in quella regione. Per verificare la regione per un bucket Amazon S3, esamina le relative proprietà nella console Amazon S3.

Per impostazione predefinita, gli archivi dati degli eventi sono crittografati da. CloudTrail È possibile utilizzare la propria chiave KMS per la crittografia quando si crea o si aggiorna un archivio dati di eventi.

Abilitazione della crittografia dei file di log

> **Note**
>
> Se crei una chiave KMS nella CloudTrail console, CloudTrail aggiunge automaticamente le sezioni relative alla politica della chiave KMS richieste. Segui queste procedure se hai creato una chiave nella console IAM o AWS CLI se devi aggiungere manualmente le sezioni della policy richieste.

Per abilitare la crittografia SSE-KMS per i file di CloudTrail registro, esegui i seguenti passaggi di alto livello:

1. Creare una chiave KMS.

- Per informazioni sulla creazione di una chiave KMS con AWS Management Console, consulta Creating Keys nella Developer Guide.AWS Key Management Service
- Per informazioni sulla creazione di una chiave KMS con AWS CLI, consulta create-key.

> **Note**
>
> La chiave KMS che scegli deve trovarsi nella stessa regione del bucket S3 che riceve i file di registro e i file digest. Per verificare la Regione per un bucket S3, verifica le relative proprietà nella console S3.

2. Aggiungi sezioni politiche alla chiave che consentono di crittografare e agli utenti di CloudTrail decrittografare i file di registro e i file digest.

   - Per ulteriori informazioni sugli elementi da includere nella policy, consulta Configura le politiche AWS KMS chiave per CloudTrail.

   > **Warning**
   >
   > Assicurati di includere le autorizzazioni di decrittografia nella politica per tutti gli utenti che devono leggere i file di registro o i file digest. Se non esegui questo passaggio prima di aggiungere la chiave alla configurazione del trail, gli utenti senza autorizzazioni di decrittografia non saranno in grado di leggere i file crittografati fino alla concessione delle suddette autorizzazioni.

   - Per informazioni sulla modifica di una policy con la console IAM, consulta Editing a Key Policy nella Guida per gli sviluppatori di AWS Key Management Service .
   - Per informazioni su come allegare una politica a una chiave KMS con, consulta. AWS CLIput-key-policy

3. Aggiorna il tuo archivio dati di percorsi o eventi per utilizzare la chiave KMS per cui hai modificato la politica. CloudTrail

   - Per aggiornare un data store di percorsi o eventi utilizzando la CloudTrail console, consultaAggiornamento di una risorsa per l'utilizzo della chiave KMS con la console.
   - Per aggiornare un data store di percorsi o eventi utilizzando il AWS CLI, vedereAbilitazione e disabilitazione della crittografia per file di CloudTrail registro, file digest e archivi di dati di eventi con AWS CLI.

CloudTrail supporta anche chiavi AWS KMS multiregionali. Per ulteriori informazioni sulle chiavi per più regioni, consulta Using multi-Region keys nella Guida per gli sviluppatori di AWS Key Management Service .

La sezione successiva descrive le sezioni della politica con cui deve essere utilizzata la politica delle chiavi KMS. CloudTrail

Concessione delle autorizzazioni per la creazione di una chiave KMS

Puoi concedere agli utenti il permesso di creare un account AWS KMS key con la `AWSKeyManagementServicePowerUser`politica.

Per concedere l'autorizzazione per creare una chiave KMS

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Scegliere il gruppo o l'utente a cui si desidera concedere l'autorizzazione.
3. Scegli la scheda Autorizzazioni.
4. Dall'elenco Aggiungi autorizzazioni, scegli Allega politiche.
5. Cerca AWSKeyManagementServicePowerUser, scegli la politica, quindi scegli Allega politiche.

   A questo punto l'utente ha l'autorizzazione per creare una chiave KMS. Per ulteriori informazioni sulla creazione di policy, consulta Creating IAM policies nella IAM User Guide.

Configura le politiche AWS KMS chiave per CloudTrail

Puoi crearne uno AWS KMS key in tre modi:

- La CloudTrail console
- La console AWS di gestione
- La AWS CLI

> **Note**
>
> Se crei una chiave KMS nella CloudTrail console, CloudTrail aggiunge la politica della chiave KMS richiesta per te. Non devi aggiungere manualmente le istruzioni della policy. Consultare Policy chiave KMS predefinita creata nella console CloudTrail .

Se crei una chiave KMS in AWS Management Console o il AWS CLI, devi aggiungere sezioni di policy alla chiave in modo da poterla utilizzare con. CloudTrail La politica deve consentire di utilizzare la chiave CloudTrail per crittografare i file di registro, i file digest e gli archivi dati degli eventi e consentire agli utenti specificati di leggere i file di registro e i file digest in formato non crittografato.

Consulta le seguenti risorse:

- Per creare una chiave KMS con, vedi create-key. AWS CLI
- Per modificare una politica chiave KMS per CloudTrail, consulta Modifica di una politica chiave nella Guida per gli sviluppatori.AWS Key Management Service
- Per dettagli tecnici sulle modalità di CloudTrail utilizzo AWS KMS, consultaCome si AWS CloudTrail usa AWS KMS.

Argomenti

- Sezioni chiave obbligatorie della policy KMS da utilizzare con CloudTrail
- Concessione delle autorizzazioni di crittografia per i percorsi
- Concessione delle autorizzazioni di crittografia per gli archivi di dati di eventi
- Concessione delle autorizzazioni di decrittografia per i sentieri
- Concessione delle autorizzazioni di decrittografia per gli archivi di dati di eventi
- Abilita CloudTrail per descrivere le proprietà della chiave KMS
- Policy chiave KMS predefinita creata nella console CloudTrail

Sezioni chiave obbligatorie della policy KMS da utilizzare con CloudTrail

Se hai creato una chiave KMS con la Console di AWS gestione o la AWS CLI, devi almeno aggiungere le seguenti istruzioni alla politica delle chiavi KMS per farla funzionare. CloudTrail

Argomenti

- Elementi della policy della chiave KMS richiesti per i trail
- Elementi della policy della chiave KMS richiesti per i datastore di eventi

Elementi della policy della chiave KMS richiesti per i trail

1. Concedi le autorizzazioni per crittografare i file di CloudTrail log e digest. Per ulteriori informazioni, consulta Concessione delle autorizzazioni di crittografia per i percorsi.

2. Concedi le autorizzazioni per CloudTrail decrittografare i file di log e digest. Per ulteriori informazioni, consulta Concessione delle autorizzazioni di decrittografia per i sentieri. Se utilizzi un bucket S3 esistente con una chiave del bucket S3, sono necessarie le autorizzazioni `kms:Decrypt` per creare o aggiornare un percorso con la crittografia SSE-KMS abilitata.
3. Abilita CloudTrail per descrivere le proprietà della chiave KMS. Per ulteriori informazioni, consulta Abilita CloudTrail per descrivere le proprietà della chiave KMS.

Come best practice per la sicurezza, aggiungi una chiave di condizione `aws:SourceArn` per la policy della chiave KMS. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che venga CloudTrail utilizzata la chiave KMS solo per uno o più percorsi specifici. Il valore di `aws:SourceArn` è sempre l'ARN del percorso (o l'array di percorsi ARNs) che utilizza la chiave KMS. Assicurarsi di aggiungere la chiave di condizione `aws:SourceArn` per le politiche chiave KMS per i percorsi esistenti.

Anche la chiave di condizione `aws:SourceAccount` è supportata, ma non consigliata. Il valore di `aws:SourceAccount` è l'ID account del proprietario del percorso o, per i percorsi organizzativi, l'ID dell'account di gestione.

> **Important**
>
> Quando aggiungi le nuove sezioni alla policy della chiave KMS, non modificare le sezioni esistenti nella policy.
> Se la crittografia è abilitata su un percorso e la chiave KMS è disabilitata o la politica della chiave KMS non è configurata correttamente CloudTrail, CloudTrail non è possibile fornire i log.

Elementi della policy della chiave KMS richiesti per i datastore di eventi

1. Concedi le autorizzazioni per crittografare un CloudTrail archivio dati di eventi Lake. Per ulteriori informazioni, consulta Concessione delle autorizzazioni di crittografia per gli archivi di dati di eventi.
2. Concedi le autorizzazioni per decrittografare un CloudTrail data store di eventi Lake. Per ulteriori informazioni, consulta Concessione delle autorizzazioni di decrittografia per gli archivi di dati di eventi.

Quando crei un datastore di eventi e lo crittografi con una chiave KMS o esegui query su un datastore di eventi che stai crittografando con una chiave KMS, dovresti avere accesso in scrittura alla chiave KMS. La policy della chiave KMS deve avere accesso a CloudTrail e la chiave KMS deve essere gestibile dagli utenti che eseguono operazioni (come le query) sul data store degli eventi.

3. Abilita CloudTrail per descrivere le proprietà della chiave KMS. Per ulteriori informazioni, consulta Abilita CloudTrail per descrivere le proprietà della chiave KMS.

Le chiavi di condizione `aws:SourceArn` e `aws:SourceAccount` non sono supportate nelle policy della chiave KMS per gli archivi di dati di eventi.

> **Important**
>
> Quando aggiungi le nuove sezioni alla policy della chiave KMS, non modificare le sezioni esistenti nella policy.
> Se la crittografia è abilitata su un archivio dati di eventi e la chiave KMS è disabilitata o eliminata o la politica della chiave KMS non è configurata correttamente CloudTrail, CloudTrail non è possibile inviare eventi al data store degli eventi.

Concessione delle autorizzazioni di crittografia per i percorsi

Example Consentono di CloudTrail crittografare i file di registro e i file digest per conto di account specifici

CloudTrail richiede l'autorizzazione esplicita per utilizzare la chiave KMS per crittografare i file di registro e i file digest per conto di account specifici. Per specificare un account, aggiungi la seguente dichiarazione obbligatoria alla politica delle chiavi KMS e *`account-id`* sostituiscila *`trailName`* con i valori appropriati per la tua configurazione. *`region`* Puoi aggiungere un altro account IDs alla `EncryptionContext` sezione per consentire a tali account di utilizzare la tua chiave KMS CloudTrail per crittografare i file di registro e i file digest.

Come best practice per la sicurezza, aggiungi una chiave di condizione `aws:SourceArn` per la policy della chiave KMS per un trail. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la chiave KMS venga CloudTrail utilizzata solo per uno o più percorsi specifici.

```
{
   "Sid": "AllowCloudTrailEncryptLogs",
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": "kms:GenerateDataKey*",
     "Resource": "*",
     "Condition": {
         "StringEquals": {
             "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
          },
          "StringLike": {
              "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
          }
     }
}
```

Example

L'esempio seguente di dichiarazione politica illustra come un altro account può utilizzare la chiave KMS per crittografare i file di CloudTrail registro e i file digest.

Scenario

- La chiave KMS si trova nell'account *111111111111*.
- Sia tu che l'account crittograferete i log*222222222222*.

Nella politica, aggiungi uno o più account che vengono crittografati con la tua chiave a. CloudTrail EncryptionContext Ciò limita CloudTrail l'utilizzo della chiave per crittografare i file di registro e i file digest solo per gli account specificati. Quando concedi alla radice dell'account l'*222222222222*autorizzazione a crittografare i file di registro e i file digest, delega l'autorizzazione all'amministratore dell'account di crittografare le autorizzazioni necessarie agli altri utenti dell'account. L'amministratore dell'account esegue questa operazione modificando le policy associate a quegli utenti IAM.

Come best practice per la sicurezza, aggiungi una chiave di condizione `aws:SourceArn` per la policy della chiave KMS. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la chiave KMS venga CloudTrail utilizzata solo per i percorsi specificati. Questa condizione non è supportata nelle policy della chiave KMS per i datastore di eventi.

Dichiarazione della policy della chiave KMS:

```
{
  "Sid": "EnableCloudTrailEncryptPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Per ulteriori informazioni sulla modifica di una politica chiave KMS da utilizzare con CloudTrail, consulta Modifica di una politica chiave nella Guida per gli AWS Key Management Service sviluppatori.

Concessione delle autorizzazioni di crittografia per gli archivi di dati di eventi

Una politica per una chiave KMS utilizzata per crittografare un archivio dati di eventi CloudTrail Lake non può utilizzare le chiavi di condizione o. `aws:SourceArn` `aws:SourceAccount` Di seguito è riportato un esempio di una policy della chiave KMS.

```
{
    "Sid": "AllowCloudTrailEncryptEds",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
```

```
}
```

Concessione delle autorizzazioni di decrittografia per i sentieri

Prima di aggiungere la chiave KMS alla CloudTrail configurazione, è importante concedere le autorizzazioni di decrittografia a tutti gli utenti che le richiedono. Gli utenti che dispongono delle autorizzazioni di crittografia ma non di quelle di decrittografia non saranno in grado di leggere i log crittografati. Se utilizzi un bucket S3 esistente con una chiave del bucket S3, sono necessarie le autorizzazioni `kms:Decrypt` per creare o aggiornare un percorso con la crittografia SSE-KMS abilitata.

Abilita le autorizzazioni di decrittografia dei log CloudTrail

Agli utenti della chiave devono essere assegnate autorizzazioni esplicite per leggere i file di log crittografati da CloudTrail . Per consentire agli utenti di leggere i log crittografati, aggiungi la seguente istruzione obbligatoria alla policy della chiave KMS, modificando la sezione `Principal` con l'aggiunta di una riga per ogni principale a cui vuoi consentire di decrittografare mediante la chiave KMS.

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Di seguito è riportato un esempio di politica necessaria per consentire al responsabile del CloudTrail servizio di decrittografare i log di percorso.

```
{
      "Sid": "AllowCloudTrailDecryptTrail",
      "Effect": "Allow",
      "Principal": {
```

```
            "Service": "cloudtrail.amazonaws.com"
          },
        "Action": "kms:Decrypt",
        "Resource": "*"
}
```

Consentire agli utenti nell'account a decrittografare i log di trail mediante la chiave KMS

Esempio

Questa istruzione della policy illustra come consentire a un utente o ruolo IAM nel tuo account di utilizzare la chiave per leggere i log crittografati nel relativo bucket S3.

Example Scenario

- La chiave KMS, il bucket S3 e l'utente IAM Bob si trovano nell'account *111111111111*.
- Concedi all'utente IAM Bob il permesso di decrittografare i CloudTrail log nel bucket S3.

Nella policy chiave, abiliti le autorizzazioni di decrittografia dei CloudTrail log per l'utente IAM Bob.

Dichiarazione della policy della chiave KMS:

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Consentire agli utenti in altri account a decrittografare i log di trail mediante la chiave KMS

Puoi consentire agli utenti di altri account di utilizzare la tua chiave KMS per decrittografare i trail log. Le modifiche da apportare alla policy della chiave variano a seconda che il bucket S3 si trovi nel tuo account o in un altro account.

Autorizzazione degli utenti di un bucket in un account diverso a decrittografare i log

Esempio

Questa istruzione della policy illustra come consentire a un utente o ruolo IAM in un altro account di utilizzare la chiave per leggere i log crittografati da un bucket S3 in un altro account.

Scenario

- La chiave KMS si trova nell'account *111111111111*.
- L'utente IAM Alice e il bucket S3 si trovano nell'account *222222222222*.

In questo caso, CloudTrail autorizzi a decrittografare i log relativi all'account e autorizzi la politica utente IAM di Alice a usare la tua chiave*222222222222*, che è nell'account. *KeyA 111111111111*

Dichiarazione della policy della chiave KMS:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:111111111111:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Istruzione della policy dell'utente IAM Alice:

JSON

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

```
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

Consentire agli utenti in un account diverso di decrittare i log di trail dal bucket

Example

Questa policy illustra come un altro account può utilizzare la tua chiave per leggere i log crittografati nel tuo bucket S3.

Example Scenario

- La chiave KMS e il bucket S3 si trovano nell'account *111111111111*.
- L'utente che leggerà i log dal bucket si trova nell'account *222222222222*.

Per abilitare questo scenario, abiliti le autorizzazioni di decrittografia per il ruolo IAM CloudTrailReadRolenel tuo account, quindi concedi all'altro account il permesso di assumere quel ruolo.

Dichiarazione della policy della chiave KMS:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
```

```
}
```

CloudTrailReadRoledichiarazione sulla politica dell'entità fiduciaria:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

Per informazioni sulla modifica di una politica chiave KMS da utilizzare con CloudTrail, consulta Modifica di una politica chiave nella Guida per gli AWS Key Management Service sviluppatori.

Concessione delle autorizzazioni di decrittografia per gli archivi di dati di eventi

Una politica di decrittografia per una chiave KMS utilizzata con un archivio dati di eventi CloudTrail Lake è simile alla seguente. L'utente o il ruolo ARNs specificato come valori per `Principal` necessita delle autorizzazioni di decrittografia per creare o aggiornare archivi di dati di eventi, eseguire query o ottenere risultati di query.

```
{
      "Sid": "EnableUserKeyPermissionsEds"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
```

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

Di seguito è riportato un esempio di politica necessaria per consentire al responsabile del CloudTrail servizio di decrittografare un archivio dati di eventi.

```
{
      "Sid": "AllowCloudTrailDecryptEds",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Abilita CloudTrail per descrivere le proprietà della chiave KMS

CloudTrail richiede la capacità di descrivere le proprietà della chiave KMS. Per abilitare questa funzionalità, aggiungi la seguente istruzione obbligatoria, senza alcuna modifica, alla policy della chiave KMS. Questa istruzione non concede CloudTrail alcuna autorizzazione oltre alle altre autorizzazioni specificate.

Come best practice per la sicurezza, aggiungi una chiave di condizione `aws:SourceArn` per la policy della chiave KMS. La chiave di condizione globale IAM `aws:SourceArn` aiuta a garantire che la chiave KMS venga CloudTrail utilizzata solo per uno o più percorsi specifici.

```
{
  "Sid": "AllowCloudTrailAccess",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Per informazioni sulla modifica delle policy della chiave KMS, consulta Editing a Key Policy nella Guida per gli sviluppatori di AWS Key Management Service .

Policy chiave KMS predefinita creata nella console CloudTrail

Se ne crei una AWS KMS key nella CloudTrail console, le seguenti politiche vengono create automaticamente. La policy supporta queste autorizzazioni:

- Consente le autorizzazioni Account AWS (root) per la chiave KMS.
- Consente di CloudTrail crittografare i file di registro e i file digest sotto la chiave KMS e di descrivere la chiave KMS.
- Consente a tutti gli utenti degli account specificati di decrittografare i file di registro e i file digest.
- Permette a tutti gli utenti nell'account specificato di creare un alias KMS per la chiave KMS.
- Abilita la decrittografia di log tra più account per l'ID account dell'account che ha creato il trail.

Argomenti

- Policy della chiave KMS predefinita per i trail
- Politica delle chiavi KMS predefinita per gli archivi di dati di eventi Lake CloudTrail

Policy della chiave KMS predefinita per i trail

Di seguito è riportato il criterio predefinito creato per un AWS KMS key che si utilizza con un trail.

> **Note**
>
> La politica include una dichiarazione per consentire a più account di decrittografare i file di registro e i file digest con la chiave KMS.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111111111111:root",
                    "arn:aws:iam::111111111111:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:trail/trail-name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
```

```
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        }
    ]
}
```

Politica delle chiavi KMS predefinita per gli archivi di dati di eventi Lake CloudTrail

La seguente è la politica predefinita creata per un AWS KMS key che utilizzi con un data store di eventi in CloudTrail Lake.

JSON

```
{
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores.
 Created ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
                "AWS": "arn:aws:iam::111111111111:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
               "AWS" : "arn:aws:sts::111111111111:assumed-role/example-role-name"
        },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
```

```
            "Resource": "*"
          }
        ]
      }
```

Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console

Sulla CloudTrail console, aggiorna un trail o un datastore di eventi per utilizzare una chiave KMS. Tieni presente che l'utilizzo della tua chiave KMS comporta AWS KMS costi di per la crittografia e la decrittografia. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.

Argomenti

- Aggiornamento di un trail per l'utilizzo di una chiave KMS
- Aggiornamento di un datastore di eventi per l'utilizzo di una chiave KMS

Aggiornamento di un trail per l'utilizzo di una chiave KMS

Per aggiornare un percorso per l'utilizzo della per AWS KMS key la quale hai modificato CloudTrail, completa i seguenti passaggi nella CloudTrail console.

> **Note**
>
> Se utilizzi un bucket S3 esistente con una chiave del bucket S3, CloudTrail devi avere l'autorizzazione nella policy della chiave per utilizzare le operazioni e. AWS KMS `GenerateDataKey` `DescribeKey` Se a `cloudtrail.amazonaws.com` non sono concesse tali autorizzazioni nella policy della chiave, non puoi creare o aggiornare un percorso.

Per aggiornare un percorso utilizzando il, consulta. AWS CLIAbilitazione e disabilitazione della crittografia per file di CloudTrail registro, file digest e archivi di dati di eventi con AWS CLI

Per aggiornare un percorso per l'utilizzo della chiave KMS

1. Accedi a AWS Management Console e apri la CloudTrail console all'indirizzo https://console.aws.amazon.com/cloudtrail/.
2. Scegli Trails (Percorsi) e quindi un nome del percorso.

3. In General details (Dettagli generali), scegli Edit (Modifica).
4. Per Log file SSE-KMS encryption (Crittografia SSE-KMS dei file di log), scegli Enabled (Abilitata) per crittografare i file di log e i file digest utilizzando la crittografia SSE-KMS anziché con SSE-S3. L'impostazione predefinita è Enabled (Abilitata). Se non abiliti la crittografia SSE-KMS, i file di log e i file digest vengono crittografati utilizzando la crittografia SSE-S3. Per ulteriori informazioni sulla crittografia SSE-KMS, consulta Utilizzo della crittografia lato server con (SSE-KMS). AWS Key Management Service Per ulteriori informazioni sulla crittografia SSE-S3, consulta Utilizzo della crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3).

   Sceglie Existing (Esistente) per aggiornare il tuo percorso con la tua AWS KMS key. Scegli una chiave KMS che si trovi nella stessa Regione del bucket S3 che riceve i file di log. Per verificare la Regione per un bucket S3, visualizza le relative proprietà nella console S3.

   > **Note**
   >
   > È anche possibile digitare l'ARN di una chiave da un altro account. Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console. La policy della chiave deve permettere di CloudTrail utilizzare la chiave per crittografare i file di log e i file digest e permettere agli utenti specificati di leggere i file di log o i file di digest in formato non crittografato. Per informazioni sulla modifica manuale della policy della chiave, consulta Configura le politiche AWS KMS chiave per CloudTrail.

   In AWS KMS Alias, specifica l'alias per il quale hai modificato la policy per l' CloudTrailutilizzo nel formato. `alias/` *`MyAliasName`* Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console.

   Puoi inserire il nome alias, l'ARN o l'ID chiave univoco a livello globale. Se la chiave KMS appartiene a un altro account, verifica che la policy della chiave disponga di autorizzazioni che ti consentano di utilizzarla. Il formato del valore può essere uno dei seguenti:

   - Nome alias: `alias/`*`MyAliasName`*
   - ARN alias: `arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - ARN chiave: `arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789012`
   - ID chiave univoco a livello globale: `12345678-1234-1234-1234-123456789012`

5. Scegli Update trail (Aggiorna percorso).

> **Note**
>
> Se la chiave KMS selezionata è disabilitata o è in attesa di eliminazione, non puoi salvare il percorso con tale chiave KMS. Puoi abilitare la chiave KMS o sceglierne un'altra. Per ulteriori informazioni, consulta Key state: Effect on your KMS key nella Guida per gli sviluppatori di AWS Key Management Service .

Aggiornamento di un datastore di eventi per l'utilizzo di una chiave KMS

Per aggiornare un datastore di eventi per AWS KMS key l'utilizzo della per la quale hai modificato CloudTrail, completa i seguenti passaggi nella CloudTrail console.

Per aggiornare un Event Data Store utilizzando il AWS CLI, vedereAggiornate un archivio dati di eventi con il AWS CLI.

> **Important**
>
> La disabilitazione o l'eliminazione della chiave KMS oppure la rimozione di CloudTrail autorizzazioni per la chiave CloudTrail impedisce di inserire eventi nell'archivio dati di eventi e impedisce agli utenti di eseguire query dei dati nell'archivio dati di eventi crittografato con la chiave. Dopo aver associato un archivio dati di eventi a una chiave KMS, la chiave KMS non può essere rimossa né modificata. Prima di disabilitare o eliminare una chiave KMS che stai utilizzando con un datastore di eventi, elimina o esegui il backup dell'archivio dati.

Aggiornamento di un datastore di eventi per l'utilizzo della chiave KMS

1. Accedi a e apri la console all'indirizzo. AWS Management Console CloudTrail https://console.aws.amazon.com/cloudtrail/
2. Nel riquadro di navigazione, seleziona Event data stores (Archivi dati di eventi) in Lake. Scegli un datastore di eventi da aggiornare.
3. In General details (Dettagli generali), scegli Edit (Modifica).
4. Per Encryption (Crittografia), se non è già abilitata, scegli Use my own AWS KMS key per crittografare il datastore di eventi con la tua chiave KMS.

Scegli Existing (Esistente) per aggiornare il datastore di eventi con la tua chiave KMS. Scegli una chiave KMS che si trovi nella stessa Regione del datastore di eventi. Una chiave di un altro account non è supportata.

In Inserisci AWS KMS alias, specifica nel formato l'alias per il quale hai modificato la policy per CloudTrail l'utilizzo. `alias/ MyAliasName` Per ulteriori informazioni, consulta Aggiornamento di una risorsa per l'utilizzo della chiave KMS con la console.

Puoi scegliere un alias o utilizzare l'ID chiave univoco globale. Il formato del valore può essere uno dei seguenti:

- Nome alias: `alias/MyAliasName`
- ARN alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- ARN chiave: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID chiave univoco a livello globale: `12345678-1234-1234-1234-123456789012`

5. Scegli Save changes (Salva modifiche).

> **Note**
>
> Se la chiave KMS selezionata è disabilitata o è in attesa di eliminazione, non puoi salvare la configurazione delil datastore di eventi con tale chiave KMS. Puoi abilitare la chiave KMS o sceglierne una diversa. Per ulteriori informazioni, consulta Key state: Effect on your KMS key nella Guida per gli sviluppatori di AWS Key Management Service .

Abilitazione e disabilitazione della crittografia per file di CloudTrail registro, file digest e archivi di dati di eventi con AWS CLI

Questo argomento descrive come abilitare e disabilitare la crittografia SSE-KMS per file di CloudTrail log, file digest e datastore di eventi utilizzando la. AWS CLI Per informazioni generali, consulta Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS).

Argomenti

- Abilitazione della crittografia per file di CloudTrail log, file digest e archivi di dati di eventi utilizzando AWS CLI
- Disattivazione della crittografia per i file di registro e i file digest utilizzando il AWS CLI

Abilitazione della crittografia per file di CloudTrail log, file digest e archivi di dati di eventi utilizzando AWS CLI

- Abilitazione della crittografia dei file di log e file digest per un trail
- Abilitazione della crittografia per un datastore di eventi

Abilita la crittografia per i file di registro e i file digest per un percorso

1. Creare una chiave con la AWS CLI. La chiave che hai creato deve fare riferimento alla stessa Regione del bucket S3 che riceve i CloudTrail file di log. Per questo passaggio, si utilizza il AWS KMS create-keycomando.
2. Ottieni la policy della chiave esistente in modo che tu possa modificarla per l'uso con CloudTrail. È possibile recuperare la politica chiave con il AWS KMS get-key-policycomando.
3. Aggiungi alla policy della chiave le sezioni necessarie in modo che gli utenti CloudTrail possano eseguire la crittografia e che gli utenti possano decrittare i file di log e digest. Assicurati che a tutti gli utenti che leggeranno i file di log vengano concesse le autorizzazioni di decrittografia. Non modificare le sezioni esistenti della policy. Per informazioni sulle sezioni della policy da includere, consulta Configura le politiche AWS KMS chiave per CloudTrail.
4. Collega il file della policy JSON modificato sulla chiave utilizzando il AWS KMS put-key-policycomando.
5. Eseguite il `update-trail` comando CloudTrail `create-trail` or con il `--kms-key-id` parametro. Questo comando consente la crittografia dei file di registro e dei file digest.

   ```
   aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
   ```

   Il parametro `--kms-key-id` specifica la chiave con la policy modificata per CloudTrail. Può avere uno qualsiasi dei seguenti formati:

   - Nome alias. Esempio: `alias/MyAliasName`
   - ARN alias. Esempio: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`

- ARN chiave. Esempio: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID chiave univoco a livello globale. Esempio: `12345678-1234-1234-1234-123456789012`

Di seguito è riportata una risposta di esempio:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

La presenza dell'`KmsKeyId`elemento indica che la crittografia dei file di registro è stata abilitata. Se la convalida dei file di registro è stata abilitata (indicata dall'`LogFileValidationEnabled`elemento impostato su true), ciò indica anche che la crittografia è stata abilitata per i file digest. I file di log e digest crittografati dovrebbero apparire nel bucket S3 configurato per il trail entro circa 5 minuti.

Abilitazione della crittografia per un datastore di eventi

1. Creare una chiave con la AWS CLI. La chiave che hai creato deve trovarsi nella stessa Regione del datastore di eventi. Per questo passaggio, esegui il AWS KMS create-keycomando.
2. Ottieni la policy della chiave esistente per modificarla per l'uso CloudTrail. Puoi ottenere la policy della chiave eseguendo il AWS KMS get-key-policycomando.
3. Aggiungi alla policy della chiave le sezioni necessarie in modo che gli utenti CloudTrail possano eseguire la crittografia e che gli utenti possano decrittare il datastore di eventi. Assicurati che a tutti gli utenti che leggeranno l'archivio dati degli eventi vengano concesse le autorizzazioni di decrittografia. Non modificare le sezioni esistenti della policy. Per informazioni sulle sezioni della policy da includere, consulta Configura le politiche AWS KMS chiave per CloudTrail.
4. Collega il file della policy JSON modificato sulla chiave eseguendo il AWS KMS put-key-policycomando.

5. Eseguite il `update-event-data-store` comando CloudTrail `create-event-data-store` or e aggiungete il `--kms-key-id` parametro. Questo comando abilitazione della crittografia dell'archivio dati degli eventi.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

Il parametro `--kms-key-id` specifica la chiave con la policy modificata per CloudTrail. Può avere uno qualsiasi dei seguenti quattro formati:

- Nome alias. Esempio: `alias/MyAliasName`
- ARN alias. Esempio: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- ARN chiave. Esempio: `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID chiave univoco a livello globale. Esempio: `12345678-1234-1234-1234-123456789012`

Di seguito è riportata una risposta di esempio:

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

La presenza dell'`KmsKeyId`elemento indica che la crittografia per l'archivio dati degli eventi è stata abilitata.

Disattivazione della crittografia per i file di registro e i file digest utilizzando il AWS CLI

Per arrestare la crittografia dei file di log e dei file digest per un trail, esegui `update-trail` e invia una stringa vuota per il `kms-key-id` parametro:

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Di seguito è riportata una risposta di esempio:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

L'assenza del `KmsKeyId` valore indica che la crittografia per file di log e file digest non è più abilitata.

> **Important**
>
> Non è possibile interrompere la crittografia per un datastore di eventi.

Come si AWS CloudTrail usa AWS KMS

Questa sezione descrive come AWS KMS funziona con un CloudTrail trail crittografato con una chiave SSE-KMS.

> **Important**
>
> AWS CloudTrail e Amazon S3 supporta solo sistemi simmetrici. AWS KMS keys Non puoi utilizzare una chiave KMS asimmetrica per crittografare i log. CloudTrail Per informazioni su come determinare se una chiave KMS è o meno asimmetrica, consulta Identifica i diversi tipi di chiavi nella Guida per gli sviluppatori di AWS Key Management Service .

Non si paga alcun costo per l'utilizzo delle chiavi quando si CloudTrail leggono o scrivono file di registro crittografati con una chiave SSE-KMS. Tuttavia, si paga un costo per l'utilizzo delle chiavi quando si accede ai file di CloudTrail registro crittografati con una chiave SSE-KMS. Per informazioni sui AWS KMS prezzi, consulta la sezione Prezzi.AWS Key Management Service Per informazioni sui prezzi di CloudTrail , consulta Prezzi di AWS CloudTrail.

Capire quando la chiave KMS viene utilizzata per il percorso

La crittografia dei file di CloudTrail registro AWS KMS si basa sulla funzionalità di Amazon S3 denominata crittografia lato server con un (SSE-KMS). AWS KMS key Per ulteriori informazioni su SSE-KMS, consulta Using server-side encryption with AWS KMS keys (SSE-KMS) nella Amazon Simple Storage Service User Guide.

Quando configuri l'utilizzo AWS CloudTrail di SSE-KMS per crittografare i tuoi file di registro e Amazon CloudTrail S3 utilizza il tuo AWS KMS keys quando esegui determinate azioni con tali servizi. Le seguenti sezioni spiegano quando e come tali servizi possono utilizzare la tua chiave KMS e forniscono informazioni aggiuntive da utilizzare per convalidare questa spiegazione.

Azioni che causano CloudTrail l'utilizzo della chiave KMS da parte di Amazon S3

- Ti configuri CloudTrail per crittografare i file di registro con il AWS KMS key
- CloudTrail inserisce un file di registro nel tuo bucket S3
- Hai a disposizione un file di log crittografato dal tuo bucket S3

Ti configuri CloudTrail per crittografare i file di registro con il AWS KMS key

Quando aggiorni la CloudTrail configurazione per utilizzare la chiave KMS, CloudTrail invia una `GenerateDataKey`richiesta AWS KMS per verificare che la chiave KMS esista e che CloudTrail sia autorizzato a utilizzarla per la crittografia. CloudTrail non utilizza la chiave dati risultante.

La richiesta `GenerateDataKey` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN del bucket S3 e il percorso in cui vengono consegnati i CloudTrail file di registro

La `GenerateDataKey` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando viene visualizzata una voce di registro come questa, è possibile determinare l' AWS KMS `GenerateDataKey`operazione CloudTrail chiamata per una traccia specifica. AWS KMS ha creato la chiave dati con una chiave KMS specifica.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T20:14:46Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770",
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
management-events",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket-123456789012-9af1fb49/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2010Z_TO50OLMG1hIQ1png.json.gz"
        }
    },
    "responseElements": null,
    "requestID": "a0555e85-7e8a-4765-bd8f-2222295558e1",
    "eventID": "e4f3557e-7dbd-4e37-a00a-d86c137d1111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770"
         }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "ce71d6be-0846-498e-851f-111a1af9078f",
    "eventCategory": "Management"
}
```

CloudTrail inserisce un file di registro nel tuo bucket S3

Ogni volta che CloudTrail inserisce un file di registro nel tuo bucket S3, Amazon S3 invia `GenerateDataKey`una richiesta AWS KMS a per conto di. CloudTrail In risposta a questa richiesta, AWS KMS genera una chiave dati univoca e quindi invia ad Amazon S3 due copie della chiave dati, una in testo semplice e una crittografata con la chiave KMS specificata. Amazon S3 utilizza la chiave dati in chiaro per crittografare il file di CloudTrail registro e quindi rimuove la chiave dati in testo semplice dalla memoria il prima possibile dopo l'uso. Amazon S3 archivia la chiave dati crittografata come metadati con il file di registro crittografato CloudTrail .

La richiesta `GenerateDataKey` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN dell'oggetto S3 (il CloudTrail file di registro)

Ogni `GenerateDataKey` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando viene visualizzata una voce di registro come questa, è possibile determinare l' AWS KMS `GenerateDataKey`operazione CloudTrail chiamata per una traccia specifica per proteggere un file di registro specifico. AWS KMS ha creato la chiave dati nella chiave KMS specificata, mostrata due volte nella stessa voce di registro.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T21:49:28Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1::trail/insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2150Z_hVXmrJzjZk2wAM2V.json.gz"
        },
```

```
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
    },
    "responseElements": null,
    "requestID": "11117d14-9232-414a-b3d1-01bab4dc9f99",
    "eventID": "999e9a50-512c-4e2a-84a3-111a5f511111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "5e663acc-b7fd-4cdd-8328-0eff862952fa",
    "eventCategory": "Management"
}
```

Hai a disposizione un file di log crittografato dal tuo bucket S3

Ogni volta che ricevi un file di CloudTrail registro crittografato dal tuo bucket S3, Amazon S3 invia `Decrypt`una richiesta AWS KMS a tuo nome per decrittografare la chiave dati crittografata del file di registro. In risposta a questa richiesta, AWS KMS utilizza la chiave KMS per decrittografare la chiave dati e quindi invia la chiave dati in testo non crittografato ad Amazon S3. Amazon S3 utilizza la chiave dati in testo semplice per decrittografare il file di CloudTrail registro e quindi rimuove la chiave dati in testo semplice dalla memoria il prima possibile dopo l'uso.

La richiesta `Decrypt` include le seguenti informazioni per il contesto di crittografia:

- L'Amazon Resource Name (ARN) del percorso CloudTrail
- L'ARN dell'oggetto S3 (il CloudTrail file di registro)

Ogni `Decrypt` richiesta genera una voce nei CloudTrail log simile all'esempio seguente. Quando viene visualizzata una voce di registro come questa, è possibile determinare che un ruolo assunto si chiama AWS KMS `Decrypt` operazione per un percorso specifico e un file di registro specifico. AWS KMS ha decrittografato la chiave dati con una chiave KMS specifica.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-12-06T22:04:04Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-12-06T22:26:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T0000Z_aAAsHbGBdye3jp2R.json.gz"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "1ab2d2d2-111a-2222-a59b-11a2b3832b53",
    "eventID": "af4d4074-2849-4b3d-1a11-a1aaa111a111",
```

```
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione per. AWS CloudTrail Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile abbonarti a un feed RSS.

- Versione API: 01-11-2013
-

Modifica	Descrizione	Data
Funzionalità aggiunta	Ora puoi registrare eventi di CloudTrail dati aggiuntivi per Amazon Aurora DSQL, Amazon Bedrock, Amazon Elastic Kubernetes Service, Amazon S3 e Amazon Keyspaces (per Apache Cassandra). Per ulteriori informazioni, consulta Data events.	1 luglio 2025
Aggiunta del supporto di un servizio	Questa versione supporta la registrazione delle chiamate API di approvazione multipart itiche. Per ulteriori informazi oni, consulta Servizi e CloudTrail integrazioni supportati.	17 giugno 2025
Funzionalità aggiunta	La registrazione delle operazioni relative agli `DeleteObject` eventi relativi ai dati di Amazon S3 ora include informazioni su tutti i singoli oggetti eliminati	9 giugno 2025

	dalla chiamata. Puoi scegliere di filtrare queste informazioni aggiuntive. Per ulteriori informazioni, consulta AWS CLI esempi di filtraggio degli eventi relativi ai dati.	
Funzionalità aggiunta	Ora puoi registrare gli eventi di attività di rete per servizi aggiuntivi. Per ulteriori informazioni, consulta Eventi di attività di rete.	30 maggio 2025
Nuove funzionalità	Ora puoi arricchire gli eventi di CloudTrail gestione e gli eventi relativi ai dati per migliorare i risultati durante la categorizzazione, la ricerca e l'analisi CloudTrail degli eventi. Per ulteriori informazioni, consulta Arricchire CloudTrail gli eventi aggiungendo chiavi di tag di risorsa e chiavi di condizione globali IAM.	29 maggio 2025
Nuove funzionalità	Sono state aggiunte informazioni sulla documentazione e sulle politiche per il ruolo collegato al `AWSServiceRoleForCloudTrailEventContext` servizio. Per ulteriori informazioni, vedere Utilizzo dei ruoli per la creazione e la gestione del contesto CloudTrail degli eventi in CloudTrail.	29 maggio 2025

Funzionalità aggiunta	È ora possibile crittografare sia i file di registro che i file digest con AWS KMS keys (SSE-KMS). Per ulteriori informazi oni, vedere Crittografia dei file di CloudTrail registro con (SSE-KMS). AWS KMS keys	22 maggio 2025
Funzionalità aggiunta	Ora puoi utilizzare selettori di eventi avanzati aggiuntivi e modelli predefiniti per registrar e gli eventi relativi ai dati sul tuo percorso. Per ulteriori informazioni, consulta Data events.	10 aprile 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi delle attività di rete per AWS Lambda Amazon Comprehen d. Per ulteriori informazioni, consulta Eventi di attività di rete.	10 aprile 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su set di configurazione, identità e-mail e modelli di Amazon Simple Email Service. Per ulteriori informazioni, consulta Data events.	10 aprile 2025
Funzionalità aggiunta	AWS CloudTrail ora supporta le policy degli endpoint VPC. Per ulteriori informazi oni, consulta Utilizzo AWS CloudTrail con gli endpoint Amazon VPC.	9 aprile 2025

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail di attività di rete per AWS IoT FleetWise.	8 aprile 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati nelle sessioni di Amazon Bedrock utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	19 marzo 2025
Documentazione aggiornata	È stato aggiornato lo schema SQL per gli eventi CloudTrail Lake Insights. Sono stati aggiunti nuovi argomenti per descrivere i campi di registrazione degli eventi di Insights per i percorsi e gli archivi di dati degli eventi. Per ulteriori informazioni sullo schema SQL supportato per gli eventi di CloudTrail Lake Insights, consulta Schema supportato per i campi dei record degli eventi di CloudTrail Insights.	13 marzo 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su applicazioni e gruppi di stream Amazon GameLift Streams utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	7 marzo 2025

Aggiunta del supporto di un servizio	Questa versione supporta le integrazioni gestite per AWS IoT Device Management. Per ulteriori informazioni, consulta Servizio AWS gli argomenti per CloudTrail.	3 marzo 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sulle applicazioni di targeting mobile di Amazon Pinpoint utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	24 febbraio 2025
Disponibilità generale degli eventi relativi alle attività di rete	Gli eventi relativi alle attività di rete sono ora disponibili a livello generale. Per ulteriori informazioni, vedere Registrazione degli eventi di attività di rete.	13 febbraio 2025
Documentazione aggiornata	È stato aggiunto l'argomento Comprendere i percorsi multiregionali e le regioni con attivazione per descrivere i percorsi multiregionali e le regioni con attivazione.	10 febbraio 2025
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sugli endpoint regionali di Amazon Timestream utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	31 gennaio 2025

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su richieste e AWS Step Functions attività di Amazon Bedrock utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	24 gennaio 2025
Documentazione aggiornata	È stato aggiunto l'argomento Optimize CloudTrail Lake queries per fornire indicazioni su come ottimizzare le query su CloudTrail Lake per migliorare le prestazioni e l'affidabilità. Questo argomento tratta tecniche di ottimizzazione specifiche e soluzioni alternative per gli errori di query più comuni.	22 gennaio 2025
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione del Messico (centrale). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	13 gennaio 2025
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Asia Pacifico (Tailandia). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	7 gennaio 2025

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati AWS Backup nei lavori di ricerca utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	30 dicembre 2024
Documentazione aggiornata	Ha convertito l'argomento sugli eventi di Logging Insights in un capitolo denominato Working with CloudTrail Insights. Il capitolo include nuove sezioni sui costi degli eventi di Insights e sulla visualizzazione degli eventi Insights per gli archivi di dati di eventi.	23 dicembre 2024
Support per IPv6	CloudTrail aggiunge il supporto per IPv6.	20 dicembre 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati durante la AWS Signer firma di lavori e profili utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	20 dicembre 2024
Documentazione aggiornata	Sezione dei servizi e delle integrazioni CloudTrail supportati aggiornata con descrizioni delle AWS Config integrazioni CloudTrail e Amazon Athena con Lake. AWS Audit Manager	18 dicembre 2024

Aggiunta del supporto di un servizio	Questa versione supporta Journeys. AWS Migration Hub Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi alla CloudTrail registrazione delle chiamate API AWS Migration Hub Journeys con. AWS CloudTrail	3 dicembre 2024
Aggiunta del supporto di un servizio	Questa versione supporta Oracle Database@AWS. Per ulteriori informazioni, vedere Servizio AWS gli argomenti relativi alla registrazione delle chiamate API CloudTrail Oracle AWS Database@ con. AWS CloudTrail	1 dicembre 2024
Aggiunta del supporto di un servizio	Questa versione supporta AWS Security Incident Response. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate API AWS Security Incident Response CloudTrail e relative alla registrazione.	1 dicembre 2024

Funzionalità aggiunta	CloudTrail Lake aggiunge il supporto per i dashboard personalizzati, la dashboard Highlights e i nuovi dashboard gestiti. Puoi creare dashboard personalizzate e aggiungere fino a 10 widget a ciascuna dashboard personalizzata. Puoi abilitare la dashboard Highlights per visualizzare una at-a-glance panoramic a dell' AWS attività raccolta dagli archivi di dati sugli eventi nel tuo account. Per ulteriori informazioni, consulta le dashboard di CloudTrail Lake.	21 novembre 2024
Funzionalità aggiunta	CloudTrail Lake aggiunge il supporto per le politiche basate sulle risorse sugli archivi di dati di eventi. È possibile utilizzare politiche basate sulle risorse per fornire l'accesso su più account per consentire ai principal i selezionati di interrogare il data store degli eventi, elencare e annullare le query e visualizzare i risultati delle query. Per ulteriori informazi oni, consulta Esempi di policy basate sulle risorse per gli archivi di dati di eventi.	21 novembre 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su AWS AppSync GraphQL APIs utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	19 novembre 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati nelle conversazioni dell' AWS IoT SiteWise Assistente utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	18 novembre 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati nei messaggi SMS di messaggistica dell'utente AWS finale utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	15 novembre 2024
Funzionalità aggiunta	È stato aggiunto il supporto per il `assumedRoot` campo `sessionContext` dell'`userIdentity` elemento. Per ulteriori informazioni, consulta CloudTrail l'elemento UserIdentity in questa guida e Track privileged tasks CloudTrail nella IAM User Guide.	14 novembre 2024

Disponibilità generale di CloudTrail Lake Query Assistant	L'assistente alle query di CloudTrail Lake è ora disponibile a livello generale. L'assistente alle interroga zioni consente di creare query SQL da istruzioni in linguaggio naturale in inglese. Per ulteriori informazioni, consulta Create CloudTrai l Lake queries from natural language prompt.	12 novembre 2024
Funzionalità aggiunta	Presentazione di una funzional ità di anteprima per le query di CloudTrail Lake che utilizza funzionalità di intelligenza artificiale generativa (IA generativa) per riepilogare i risultati delle query. Per ulteriori informazioni, consulta Riepilogare i risultati delle query in linguaggio naturale.	12 novembre 2024

Funzionalità aggiunta	Ora puoi configurare campi di selezione degli eventi avanzati aggiuntivi per i data store di eventi di CloudTrai l Lake, il che ti offre un maggiore controllo sugli CloudTrail eventi da inserire nei tuoi archivi di dati di eventi. Puoi filtrare gli eventi di gestione nei seguenti campi avanzati di selezione degli eventi: `eventName` (nuovo)`eventSour ce` , `eventType` (nuovo)`readOnly`, `sessionCredentialF romConsole` (nuovo) e `userIdentity.arn` (nuovo). È possibile filtrare gli eventi di dati nei seguenti campi avanzati di selezione degli eventi:`eventName` , `eventSource` `eventType` (nuovo),`resources.type` , `resources.ARN` `readOnly`, `sessionCredentialF romConsole` (nuovo) e `userIdentity.arn` (nuovo). Per ulteriori informazi oni, consulta Creare un archivio dati di CloudTrail eventi per gli eventi con la console (passaggi 16 e 17).	11 novembre 2024

Versione aggiornata dell'evento	`inScopeOf` Campo `eventVersion` aggiornato `1.11` e aggiunto per l'`userIdentity` elemento. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .	29 ottobre 2024
Aggiunta del supporto di un servizio	Questa versione supporta la messaggistica SMS per l'utente AWS finale. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate API SMS di messaggistica con l'utente AWS finale. CloudTrail	22 ottobre 2024
Funzionalità aggiunta	È ora possibile registrare gli eventi CloudTrail relativi ai dati sulle identità di origine degli SMS di AWS End User Messaging utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	22 ottobre 2024
Aggiunta del supporto di un servizio	Questa versione supporta AWS End User Messaging Social. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate dell'API social di messaggistica AWS finale per CloudTrail l'utente finale.	10 ottobre 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sul numero di telefono di AWS End User Messaging Social IDs utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	10 ottobre 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su modelli e AWS Data Exchange asset Amazon Bedrock utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	27 settembre 2024

Funzionalità aggiunta	Ora puoi configurare percorsi e archivi dati di eventi per registrare gli eventi delle attività di CloudTrail rete (in anteprima). Gli eventi di attività di rete consentono ai proprietari di endpoint VPC di registrare le chiamate AWS API effettuate utilizzando i propri endpoint VPC da un VPC privato a. Servizio AWS Questa versione supporta la registrazione degli eventi delle attività di rete per le seguenti fonti di eventi:,, e. `cloudtrail.amazonaws.com` `ec2.amazonaws.com` `kms.amazonaws.com` `secretsmanager.amazonaws.com` Per ulteriori informazioni, vedere Registrazione degli eventi delle attività di rete.	24 settembre 2024
Aggiunta del supporto di un servizio	Questa versione supporta AWS Directory Service Data. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate API AWS Directory Service Data Logging. CloudTrail	18 settembre 2024

Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Asia Pacifico (Malesia). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	22 agosto 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui monitor delle app Amazon CloudWatch RUM utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	25 luglio 2024
Funzionalità aggiunta	Ora puoi controllare l'accesso ai percorsi utilizzando i tag. Per ulteriori informazioni, consulta ABAC with CloudTrail.	23 luglio 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sugli utenti di Amazon One Enterprise e UKeys utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	23 luglio 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su alias e guardrail di flusso di Amazon Bedrock e l'attività delle API a livello di oggetto di Amazon S3 sui bucket di directory utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	9 luglio 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su AWS Payment Cryptogra phy chiavi e alias utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	5 luglio 2024
Funzionalità aggiunta	Presentazione di una funzional ità di anteprima per le query di CloudTrail Lake che utilizza funzionalità di intelligenza artificiale generativa (AI generativa) per produrre una query SQL da un prompt in lingua inglese. Per ulteriori informazioni, consulta Creare query CloudTrail Lake da istruzioni in lingua inglese.	11 giugno 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su CloudWatch parametri Amazon, modelli Amazon Machine Learning ML e AWS Private CA utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	5 giugno 2024
Documentazione aggiornata	È stata aggiunta una sezione per descrivere come filtrare gli eventi di dati utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Filtrare gli eventi di dati utilizzando selettori di eventi avanzati.	29 maggio 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui flussi di Amazon Kinesis Data Streams e trasmette re i consumatori utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	21 maggio 2024
Documentazione aggiornata	È stata aggiornata la pagina delle regioni supportate dai CloudTrail laghi per aggiunger e la regione Asia Pacifico (Hyderabad) (ap-south-2), la regione Europa (Zurigo) (eu-central-2) e la regione Israele (Tel Aviv) (il-central-1).	16 maggio 2024

Funzionalità aggiunta	È ora possibile registrar e gli eventi relativi ai dati sulle macchine a stati utilizzando selettori di eventi avanzati. CloudTrail AWS Step Functions Per ulteriori informazioni, consulta Data events.	16 maggio 2024
Documentazione aggiornata	È stata aggiunta una sezione sulla visualizzazione CloudTrai l dei costi e dell'utilizzo utilizzando AWS Cost Explorer. Per ulteriori informazi oni, consulta Visualizzazione dei CloudTrail costi e dell'util izzo con AWS Cost Explorer.	14 maggio 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su Amazon Q Apps utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	1º maggio 2024

Documentazione aggiornata	Miglioramenti organizzativi generali alle sezioni della guida per l'utente e ai titoli delle pagine, tra cui: il titolo della pagina di riferimento degli eventi di CloudTrail registro è stato modificato in Understanding CloudTrail events e sono state aggiunte descrizioni degli eventi di gestione, degli eventi relativi ai dati e degli eventi Insights. Titolo modificato della pagina Impostazioni in Configura CloudTrail impostazioni. Le pagine Logging data events, Logging management events e Logging Insights events sono state spostate nella sezione Understanding CloudTrail events. La pagina di esempi di file di CloudTrail registro è stata spostata nella sezione dei file di CloudTrail registro. Sono state aggiunte pagine separate per elencare i AWS CLI comandi per gli archivi di dati degli eventi, le query e le integrazioni di CloudTrail Lake.	10 aprile 2024
Documentazione aggiornata	È stata aggiornata la pagina delle regioni supportate dai CloudTrail laghi per aggiunger e la regione Europa (Spagna) (eu-south-2).	10 aprile 2024

Aggiunta del supporto di un servizio	Questa versione supporta AWS Control Catalog. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate API di AWS Control Catalog CloudTrail e della registrazione.	8 aprile 2024
Aggiunta del supporto di un servizio	Questa versione supporta AWS Deadline Cloud. Per ulteriori informazioni, consulta Servizio AWS gli argomenti per CloudTrail.	2 aprile 2024
Versione aggiornata dell'evento	La versione AWS CloudTrail dell'evento è ora 1.10. Per ulteriori informazioni, consulta il contenuto del CloudTrail record.	26 marzo 2024
Aggiunta del supporto di un servizio	Questa release supporta AWS Billing Conductor. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo CloudTrail AWS CloudTrail e alla registrazione delle chiamate AWS Billing Conductor API.	12 marzo 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su AWS X-Ray tracce e nodi AWS Systems Manager gestiti utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	7 marzo 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui domini Amazon Simple Workflow Service (Amazon SWF) utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	14 febbraio 2024
Funzionalità aggiunta	CloudTrail ha aggiunto l'`ListInsightsMetricData` API. L'`ListInsightsMetricData` API restituisce i dati delle metriche di Insights per i percorsi che hanno abilitato Insights. Per ulteriori informazioni, consulta ListInsightsMetricData nella documentazione di riferimento dell'API AWS CloudTrail .	6 febbraio 2024
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati per AWS IoT e AWS AppConfig utilizzando selettori di eventi avanzati. AWS IoT SiteWise Per ulteriori informazioni, consulta Data events.	4 gennaio 2024

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati AWS IoT Greengrass utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	22 dicembre 2023
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Canada occidentale (Calgary) . Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	20 dicembre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati per Amazon Keyspaces (per Apache Cassandra), AWS IoT TwinMaker Amazon RDS e Catena di approvvigionamento di AWS utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Data events.	20 dicembre 2023
Politica AWS gestita aggiornata	La policy gestita CloudTrailServiceRolePolicy è stata aggiornata per consentire le seguenti operazioni in un datastore di eventi dell'organizzazione quando la federazione è disabilitata: `glue:DeleteTable` e `lakeformation:DeregisterResource` .	26 novembre 2023

Funzionalità aggiunta	Ora puoi federare un data store di eventi CloudTrail Lake per visualizzare i metadati associati al data store di eventi nel Data Catalog ed eseguire query SQL sui AWS Glue dati dell'evento utilizzando Amazon Athena. I metadati delle tabelle archiviati nel AWS Glue Data Catalog consenton o al motore di query Athena di sapere come trovare, leggere ed elaborare i dati che desideri interrogare. Per ulteriori informazioni, consulta Federazione di un datastore di eventi.	26 novembre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati AWS Cloud Map utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	16 novembre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui messaggi Amazon SQS utilizzando selettori di eventi avanzati. Per ulteriori informazi oni, consulta Registrazione degli eventi di dati.	16 novembre 2023

Funzionalità aggiunta	CloudTrail Lake offre ora due opzioni di prezzo per gli archivi di dati di eventi: prezzi di conservazione estendibili per un anno e prezzi di conservazione per sette anni. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Prima di questa versione, tutti i datastore di eventi utilizzavano l'opzione di prezzo per la conservazione di sette anni. È possibile passare dall'utilizzo dell'opzione di prezzo di conservazione di sette anni a quella estendibile di un anno per un datastore di eventi utilizzando la console o il funzionamento dell'API. CloudTrail AWS CLIUpdateEventDataStore Per ulteriori informazioni sulle opzioni di prezzo, consulta Prezzo AWS CloudTrail e Opzioni di prezzo del datastore di eventi.	15 novembre 2023

Funzionalità aggiunta	Ora puoi raccogliere eventi Insights in Lake. CloudTrail AWS CloudTrail Insights aiuta AWS gli utenti a identificare e rispondere alle attività insolite associate alle frequenze di chiamata e ai tassi di errore delle API analizzan do continuamente gli eventi di CloudTrail gestione. Per raccogliere gli eventi di Insights in CloudTrail Lake, è necessario un data store di eventi di origine che registri gli eventi di gestione e abiliti Insights e un data store di eventi di destinazione che raccolga gli eventi Insights in base ad attività di gestione insolite nell'archivio dati degli eventi di origine. Per ulteriori informazioni, consulta Creare un archivio dati di eventi per gli eventi di CloudTrail Insights e Logging Insights.	9 novembre 2023
Aggiunta del supporto di un servizio	Questa release supporta AWS Launch Wizard. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo CloudTrail e alla registrazione delle chiamate AWS Launch Wizard API. AWS CloudTrail	8 novembre 2023

Aggiunta del supporto di un servizio	Questa versione supporta Amazon Bedrock. Per ulteriori informazioni, consulta Servizio AWS gli argomenti CloudTrail e registra le chiamate API Amazon Bedrock utilizzando AWS CloudTrail.	23 ottobre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sulle CodeWhisperer personalizzazioni di Amazon utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	18 ottobre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su database e tabelle Amazon Timestream utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	28 settembre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su argomenti e endpoint della piattaforma Amazon SNS utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	28 settembre 2023

Documentazione aggiornata	È stata aggiunta una tabella per mostrare le attività che possono eseguire l'account di gestione, gli account amministratore delegato e gli account dei membri all'inter no di un' AWS Organizations organizzazione. CloudTrail Per ulteriori informazioni, consulta Amministratore delegato di un'organizzazione.	25 settembre 2023
Aggiunta del supporto di un servizio	Questa versione supporta Marketplace AWS gli accordi. Per ulteriori informazioni, consulta Servizio AWS gli argomenti relativi all'utilizzo AWS CloudTrail delle chiamate API di Agreements. CloudTrail	1 settembre 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui flussi video di Amazon Kinesis e sugli endpoint Amazon SageMaker AI utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	31 agosto 2023

Aggiunta del supporto di un servizio	Questa versione supporta AWS Application Transformation Service. AWS Application Transformation Service è un servizio di back-end utilizzato da servizi come AWS Microservice Extractor for .NET. Per ulteriori informazioni, consulta i servizi e le integrazioni CloudTrail supportati.	26 agosto 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su AWS Private CA Connector for Active Directory utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	24 agosto 2023
Documentazione aggiornata	Sono stati aggiunti nuovi scenari CloudTrail Lake per mostrare come creare archivi di dati di eventi, visualizzare i dashboard di CloudTrail Lake, copiare gli eventi di trail in un data store di eventi, visualizzare ed eseguire query di esempio e salvare i risultati delle query in un bucket Amazon S3 utilizzando il. AWS Management ConsolePer ulteriori informazioni, consulta Scenari per Lake CloudTrail	16 agosto 2023

Supporto di una nuova Regione	CloudTrail ha esteso il sostegno a una nuova regione, la regione di Israele (Tel Aviv). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	1° agosto 2023
Aggiunta del supporto di un servizio	Questa release supporta AWS HealthImaging. Per ulteriori informazioni, consulta Servizi e integrazioni CloudTrail supportati e Utilizzo delle chiamate AWS HealthImaging API di registrazione. AWS CloudTrail	26 luglio 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati negli archivi AWS HealthIma ging dati utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	26 luglio 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui canali AWS Systems Manager di controllo e sulle reti Amazon Managed Blockchain utilizzan do selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	21 giugno 2023

Funzionalità aggiunta	Ora puoi verificare i risultati delle query salvate su CloudTrail Lake utilizzando il aws cloudtrail verify-query-results comando. Per ulteriori informazioni, consulta Convalida dei risultati delle query salvate con la AWS CLI.	21 giugno 2023
Aggiunta del supporto di un servizio	Questa versione supporta Autorizzazioni verificate da Amazon. Per ulteriori informazioni, consulta i servizi e le integrazioni CloudTrail supportati e l'utilizzo di chiamate API Amazon Verified Permissions. AWS CloudTrail	13 giugno 2023
Funzionalità aggiunta	Ora puoi utilizzare le dashboard di CloudTrail Lake per visualizzare gli eventi in un archivio dati di eventi. Per ulteriori informazioni, consulta Visualizzazione dei pannelli di controllo di Lake.	13 giugno 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati negli archivi di policy di Amazon Verified Permissions utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	13 giugno 2023

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su un CodeWhisperer profilo Amazon utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	6 giugno 2023
Funzionalità aggiunta	Ora puoi avviare e interrompere l'acquisizione di eventi negli archivi di dati CloudTrail degli eventi. Per informazioni su come interrompere l'importazione di eventi tramite la console, consulta Impedire a un datastore di eventi di importare gli eventi. Per informazioni su come interrompere l'inserimento di eventi utilizzando il AWS CLI, consultate Interrompere l'ingestione su un data store di eventi.	2 giugno 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su un'area di lavoro write-ahead log di Amazon EMR utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	31 maggio 2023

Aggiunta del supporto di un servizio	Questa versione supporta Amazon Security Lake. Per ulteriori informazioni, consulta Servizi e integrazioni CloudTrail supportati e Registrazione delle chiamate API di Amazon Security Lake tramite. AWS CloudTrail	30 maggio 2023
Versione aggiornata dell'evento	Ora `eventVersion` è 1.09.	23 maggio 2023
Documentazione aggiornata	Argomento CloudTrail dell'elemento UserIdentity aggiornato per includere un esempio e le descrizioni dei campi per una richiesta effettuata per conto di un utente di IAM Identity Center. Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .	23 maggio 2023
Documentazione aggiornata	Questo aggiornamento supporta la seguente versione di patch per la CloudTrai l Processing Library: aws-cloudtrail-processing-l ibrary -1.6.1.jar. Per ulteriori informazioni, vedere Using the CloudTrail Processing Library e Processing Library onCloudTrail. GitHub	23 maggio 2023

Funzionalità aggiunta	CloudTrail Lake ora supporta tutte le funzioni e gli operatori Presto. Per ulteriori informazioni, consulta i vincoli di CloudTrail Lake SQL.	9 maggio 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati su un GuardDuty rilevatore Amazon utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi dei dati e Registrazione delle chiamate GuardDuty API Amazon con. AWS CloudTrail	30 marzo 2023
Documentazione aggiornata	È stata aggiunta una nuova sezione sulla creazione di tag di allocazione dei costi definiti dall'utente per i datastore di eventi. Per ulteriori informazioni, consulta Creazione di tag di allocazione dei costi definiti dall'utente per i data store di eventi CloudTrail Lake.	24 marzo 2023
Aggiunta del supporto di un servizio	Questa versione supporta AWS Telco Network Builder (TNB).AWS Per ulteriori informazioni, consulta Servizi e integrazioni CloudTrail supportati e Registrazione delle chiamate API AWS Telco Network Builder tramite. AWS CloudTrail	21 febbraio 2023

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui pool di identità di Amazon Cognito utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	15 febbraio 2023
Documentazione aggiornata	È stata aggiunta una nuova sezione sulle risorse didattiche disponibili per CloudTrail Lake. Per ulteriori informazioni, consulta la sezione Risorse didattiche.	9 febbraio 2023
Funzionalità aggiunta	Ora puoi creare integrazioni CloudTrail Lake con fonti di AWS eventi esterne a. Puoi registrare e archiviar e i dati delle attività degli utenti da qualsiasi origine nei tuoi ambienti ibridi, ad esempio applicazioni interne o SaaS ospitate on-premis e o nel cloud, macchine virtuali o container. Per ulteriori informazioni, consulta Creazione di un'integrazione con un'origine di eventi esterna ad AWS.	31 gennaio 2023

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati relativi CloudTrail `PutAuditEvents` all'attività su un canale CloudTrail Lake utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	31 gennaio 2023
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Asia Pacifico (Melbourne). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	24 gennaio 2023
Documentazione aggiornata	È stata aggiunta una nuova sezione sulla gestione della coerenza dei dati in CloudTrail, vedere Gestione della coerenza dei dati in CloudTrail.	18 gennaio 2023
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui feature store di Amazon SageMaker AI utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	27 dicembre 2022
Aggiunta del supporto di un servizio	Questa versione supporta Marketplace AWS Discovery. Consulta Servizi e integrazioni AWS CloudTrail supportati.	15 dicembre 2022

Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sui componenti di prova degli esperimenti di Amazon SageMaker AI Metrics utilizzan do selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	15 dicembre 2022
Funzionalità aggiunta	Ora puoi creare un Event Data Store per includere elementi di AWS Config configurazione e utilizzare l'Event Data Store per esaminare le modifiche non conformi ai tuoi ambienti di produzione. Per ulteriori informazioni, consulta Creare un event data store per AWS Config gli elementi di configura zione.	28 novembre 2022
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Asia Pacifico (Hyderabad). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	22 novembre 2022
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati Amazon FinSpace negli ambienti utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	18 novembre 2022

Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Europa (Spagna). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	16 novembre 2022
Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Europa (Zurigo). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	9 novembre 2022
Funzionalità aggiunta	L'account di gestione di un' AWS Organizations organizzazione può ora aggiungere un amministratore delegato per gestire i CloudTrail percorsi e gli archivi di dati degli eventi dell'organizzazione. Per ulteriori informazioni, consulta Amministratore delegato di un'organizzazione.	7 novembre 2022
Funzionalità aggiunta	Ora puoi abilitare AWS Key Management Service la crittografia per un archivio dati di eventi CloudTrail Lake. Per ulteriori informazioni, consulta Creazione di un datastore di eventi.	7 novembre 2022

Funzionalità aggiunta	Ora puoi salvare i risultati delle query di CloudTrail Lake in un bucket Amazon S3 quando esegui una query. Per ulteriori informazioni sull'esecuzione di una query, consultare Eseguire una query e salvare i risultati della query. Per ulteriori informazioni sul download dei risultati della query, consultare Ottenere e scaricare i risultati della query salvati.	21 ottobre 2022
Funzionalità aggiunta	Ora puoi copiare gli eventi del CloudTrail trail in un data store di eventi CloudTrail Lake. Per ulteriori informazioni, consulta Copiare gli eventi del trail su CloudTrail Lake.	19 settembre 2022
Documentazione aggiornata	È stato aggiunto un elenco di CloudWatch metriche Amazon supportate per CloudTrail Lake. Per ulteriori informazi oni, consulta CloudWatch Metriche supportate.	16 settembre 2022
Funzionalità aggiunta	È ora possibile visualizzare i canali CloudTrail collegati ai servizi utilizzando il. AWS CLI Per ulteriori informazi oni, vedere Visualizzazione dei canali collegati ai servizi utilizzando il CloudTrail . AWS CLI	9 settembre 2022

Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione del Medio Oriente (Emirati Arabi Uniti). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	30 agosto 2022
Funzionalità modificate	CloudTrail ha cambiato il nome della politica gestita `AWSCloudTrailReadOnlyAccess` in `AWSCloudTrail_ReadOnlyAccess`. Le autorizzazioni in questa policy sono state ancorate. Per impostazione predefinita, la policy non concede più l'autorizzazione a elencare tutti i bucket AWS Lambda , le funzioni o gli alias di Amazon S3. AWS KMS Per ulteriori informazioni, consulta Accesso in sola lettura.	6 giugno 2022
Funzionalità modificate	Come best practice per la sicurezza, ora puoi aggiungere una chiave di condizione `aws:SourceArn` o `aws:SourceAccount` a un blocco di verifica ACL `s3:GetBucketAcl` nelle policy di bucket Amazon S3. Per ulteriori informazioni, consulta Configurare le policy dei bucket di Amazon S3 per. CloudTrail	11 maggio 2022

Funzionalità modificate	A partire dal 24 febbraio 2022, AWS CloudTrail ha iniziato a modificare i valori dei `sourceIPAddress` campi `userAgent` e, in ogni caso, quelli originati da una AWS Management Console sessione in cui veniva utilizzat o un client proxy. Per questi eventi, CloudTrail sostituisce i valori dei campi `userAgent` e `sourceIPAddress` con. `AWS Internal` CloudTrai lha apportato questa modifica per standardizzare il modo in cui registra le informazi oni per le azioni di servizio su tutti i servizi. AWS Per ulteriori informazioni, consulta il contenuto del CloudTrail record.	12 aprile 2022
Aggiunta del supporto di un servizio	Questa versione supporta Amazon GameSparks. Consulta Servizi e integrazioni AWS CloudTrail supportati.	24 marzo 2022
Aggiunta del supporto di un servizio	Questa versione supporta AWS App Mesh Envoy Management Service. Consulta Servizi e integrazioni AWS CloudTrail supportati.	18 marzo 2022

Documentazione aggiornata	Sono stati aggiunti nuovi esempi di query per CloudTrail Lake, una nuova funzionalità che consente di eseguire query SQL granulari e multicampo sui propri eventi. Inoltre, un nuovo campo, `BytesScanned`, è stato aggiunto ai risultati dei metadati della query di `DescribeQuery` e operazioni `GetQueryResults`. Per ulteriori informazioni, consulta Working with Lake. CloudTrail	4 marzo 2022
Funzionalità modificate	CloudTrail ora rimuove l'ID account del proprietario del bucket Amazon S3 nel `resources` blocco di un evento dati se vengono soddisfatte entrambe le seguenti condizioni: la chiamata API dell'evento dati proviene da un AWS account diverso dal proprietario del bucket Amazon S3 e il chiamante dell'API ha ricevuto un `AccessDenied` errore relativo solo all'account chiamante. Per ulteriori informazioni, consulta Redacting dell'account del proprietario del bucket per gli eventi di dati richiamati da altri account IDs.	3 marzo 2022

Documentazione aggiornata	Questo aggiornamento supporta la seguente versione per la CloudTrail Processin g Library: è stato aggiunto il supporto per l'impleme ntazione di un gestore S3 personalizzato, la registraz ione degli eventi per le eccezioni relative all'analisi dei file di registro, il supporto per l'analisi di un `errorCode` campo opzionale e l'aggiorn amento dell'espressione regolare di analisi degli ID dell'account per `insightDe tails` accettare valori non numerici. Per ulteriori informazioni, consulta Using the Processing Library e Processing Library on. CloudTrail CloudTrail GitHub	28 gennaio 2022
Funzionalità aggiunta	CloudTrail presenta CloudTrai l Lake, una nuova funzional ità che consente di eseguire query SQL a più campi e granulari sui propri eventi. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. Per ulteriori informazioni, consulta Working with Lake. CloudTrail	5 gennaio 2022

Supporto di una nuova Regione	CloudTrail supporto esteso a una nuova regione, la regione Asia-Pacifico (Giacarta). Per ulteriori informazioni, consulta Regioni CloudTrail supportate.	13 dicembre 2021
Aggiunta del supporto di un servizio	Questa versione supporta Amazon WorkSpaces Web. Consulta Servizi e integrazioni AWS CloudTrail supportati.	3 dicembre 2021
Funzionalità aggiunta	Ora puoi registrare gli eventi CloudTrail relativi ai dati sulle AWS Glue tabelle create da Lake Formation utilizzando selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	30 novembre 2021
Funzionalità modificate	Come best practice di sicurezza, ora puoi aggiunger e una chiave di `aws:SourceAccount` condizione `aws:SourceArn` or alle policy chiave e alle AWS KMS policy dei bucket di Amazon S3. Per ulteriori informazi oni, consulta Configurare le politiche AWS KMS chiave per CloudTrail e Configurare le politiche dei bucket Amazon S3 per. CloudTrail	15 novembre 2021

Aggiunta del supporto di un servizio	Questa versione supporta AWS Resilience Hub. Consulta Servizi e integrazioni AWS CloudTrail supportati.	10 novembre 2021
Funzionalità aggiunta	È disponibile un nuovo tipo di evento CloudTrail Insights: tasso di errore degli eventi Insights. Un evento Insights relativo al tasso di errore rileva un'attività insolita dovuta a un errore che si verifica quando l'account APIs viene richiamat o. Per ulteriori informazioni, consultare Registrazione di eventi Insight per i trail.	10 novembre 2021
Funzionalità aggiunta	È ora possibile registrare gli eventi CloudTrail relativi ai dati sui flussi DynamoDB utilizzan do selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	22 settembre 2021
Funzionalità aggiunta	Ora puoi registrare eventi di dati sui punti di accesso Amazon S3. Puoi registrar e eventi di dati di access point Amazon S3 utilizzando i selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	24 agosto 2021

Funzionalità modificate	Quando configuri un trail per inviare notifiche ad Amazon SNS, CloudTrail aggiunge una dichiarazione di policy alla policy di accesso agli argomenti SNS che consente di inviare contenuti CloudTrai l a un argomento SNS. Come best practice di sicurezza, consigliamo di aggiungere una chiave di `aws:Sourc eAccount` condizione `aws:SourceArn` or alla CloudTrail dichiarazione di policy. Per ulteriori informazi oni, consulta la policy tematica di Amazon SNS per. CloudTrai l	16 agosto 2021
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Route 53 Application Recovery Controller. Consulta Servizi e integrazioni AWS CloudTrail supportati.	27 luglio 2021
Funzionalità aggiunta	Ora puoi registrare gli eventi relativi ai dati su Amazon EBS direct APIs run on EBS snapshot EBS. Puoi registrare eventi di dati delle API dirette di Amazon EBS utilizzando i selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	27 luglio 2021

Funzionalità modificate	Quando CloudTrail elabora gli eventi relativi ai dati, conserva i numeri nel loro formato originale, che si tratti di un numero intero () o di un. `int` `float` Negli eventi che contengono numeri interi nei campi di un evento di dati, CloudTrail storicamente elaborava questi numeri come float. Ora, CloudTrail mantiene il formato originale dei numeri interi negli eventi di dati. Per ulteriori informazioni, consulta Using the CloudTrail Processing Library.	13 luglio 2021
Funzionalità aggiunta	Ora puoi escludere gli eventi di gestione delle API dati di Amazon RDS dai percorsi. Per ulteriori informazioni, consulta Registrazione di eventi di gestione per i percorsi.	1° luglio 2021
Aggiunta del supporto di un servizio	Questa release supporta AWS BugBust. Consulta Servizi e integrazioni AWS CloudTrail supportati.	24 giugno 2021
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Managed Grafana e Amazon Managed Service for Prometheus. Consulta Servizi e integrazioni AWS CloudTrail supportati.	2 giugno 2021

Aggiunta del supporto di un servizio	Questa versione supporta AWS App Runner. Consulta Servizi e integrazioni AWS CloudTrail supportati.	18 maggio 2021
Aggiunta del supporto di un servizio	Questa versione supporta AWS Systems Manager Incident Manager. Consulta Servizi e integrazioni AWS CloudTrail supportati.	10 maggio 2021
Documentazione aggiornata	Questo aggiornamento descrive i requisiti di registrazione degli eventi dei dati per i pacchetti di AWS Config conformità, in particolare per i framework di conformità come HIPAA o FedRAMP. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	7 maggio 2021
Aggiunta del supporto di un servizio	Questa versione supporta Service Quotas e Amazon EBS direct. APIs Consulta Servizi e integrazioni AWS CloudTrail supportati.	13 aprile 2021

Funzionalità aggiunta	Dopo la configurazione AWS STS, un amministratore IAM CloudTrail registra `sourceIdentity` le informazioni negli eventi in cui gli utenti assumono un ruolo IAM o eseguono azioni con il ruolo assunto. Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.	13 aprile 2021
Documentazione aggiornata	Questo aggiornamento documenta i limiti, in kilobyte (KB), per il contenuto di alcuni CloudTrail campi di registrazione degli eventi. Per ulteriori informazioni, consulta il contenuto dei CloudTrail record.	8 aprile 2021
Funzionalità aggiunta	Dopo la configurazione AWS STS, un amministratore IAM CloudTrail registra `sourceIdentity` le informazioni negli eventi quando gli utenti assumono un ruolo IAM o eseguono azioni con il ruolo assunto. Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.	6 aprile 2021

Funzionalità aggiunta	Ora puoi registrare gli eventi di dati nelle tabelle Amazon DynamoDB. Puoi registrar e eventi di dati Dynamo DB utilizzando selettori di eventi o selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	23 marzo 2021
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Managed Workflows for Apache Airflow. Consulta Servizi e integrazioni AWS CloudTrail supportati.	22 marzo 2021
Funzionalità aggiunta	Ora puoi registrare gli eventi di dati sui punti di accesso Lambda di oggetti S3 se hai scelto di utilizzare selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	18 marzo 2021
Aggiunta del supporto di un servizio	Questa versione supporta AWS Fault Injection Simulator. Consulta Servizi e integrazioni AWS CloudTrail supportati.	15 marzo 2021

Funzionalità aggiunta	Ora puoi registrare eventi di dati sui nodi Ethereum in Blockchain gestita da Amazon se hai scelto di utilizzare selettori di eventi avanzati. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	1° marzo 2021
Aggiunta del supporto di un servizio	Questa versione supporta Blockchain gestita da Amazon e l'anteprima di Ethereum per Managed Blockchain. Consulta Servizi e integrazioni AWS CloudTrail supportati.	4 febbraio 2021
Aggiunta del supporto di un servizio	Questa release supporta AWS Amplify. Consulta Servizi e integrazioni AWS CloudTrail supportati.	3 febbraio 2021
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Lookout for Metrics. Consulta Servizi e integrazioni AWS CloudTrail supportati.	1° febbraio 2021

Documentazione aggiornata	Questo aggiornamento supporta la seguente versione di patch per la CloudTrail Processing Library: Aggiorna i riferimenti ai file.jar nella guida per l'utente per utilizzar e la versione più recente, aws-cloudtrail-processing-l ibrary -1.4.0.jar. Per ulteriori informazioni, vedere Using the CloudTrail Processing Library e Processing Library on. CloudTrail GitHub	12 gennaio 2021
Funzionalità aggiunta	Ora puoi registrare eventi di dati su Amazon S3 su AWS Outposts. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	21 dicembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Lookout for Equipment AWS Well-Arch itected Tool e Amazon Location Service. Consulta Servizi e integrazioni AWS CloudTrail supportati.	16 dicembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta AWS IoT Greengrass la versione 2. Consulta Servizi e integrazioni AWS CloudTrail supportati.	15 dicembre 2020

Aggiunta del supporto di un servizio	Questa versione supporta Amazon EMR su EKS. Consulta Servizi e integrazioni AWS CloudTrail supportati.	10 dicembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta AWS Audit Manager e Amazon HealthLake. Consulta Servizi e integrazioni AWS CloudTrail supportati.	8 dicembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Lookout for Vision. Consulta Servizi e integrazioni AWS CloudTrail supportati.	1° dicembre 2020
Versione aggiornata dell'evento	La versione AWS CloudTrail dell'evento è ora 1.08. La versione 1.08 introduce nuovi campi per. CloudTrail Per ulteriori informazioni, consulta il contenuto del CloudTrail record.	24 novembre 2020

Funzionalità aggiunta	AWS CloudTrail introduce selettori di eventi avanzati per gli eventi di dati. I selettori di eventi avanzati consentono un controllo più dettagliato degli eventi di dati che registri nel percorso. È possibile includere o escludere eventi relativi ai dati per AWS risorse specifich e e selezionarne di specifici APIs per accedere al percorso. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	24 novembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta AWS Network Firewall. Consulta Servizi e integrazioni AWS CloudTrail supportati.	17 novembre 2020
Aggiunta del supporto di un servizio	Questa versione supporta AWS Trusted Advisor. Consulta Servizi e integrazioni AWS CloudTrail supportati.	22 ottobre 2020
Documentazione aggiornata	Sono stati aggiunti due nuovi esempi di record di eventi per gli eventi di accesso dell'utente root. Per ulteriori informazioni, consulta Eventi di accesso alla console AWS.	13 ottobre 2020

Funzionalità modificate	Le autorizzazioni nella policy di `AWSCloudTrail_FullAccess` sono state ristrette. Questa policy non ti permette più di eliminare gli argomenti di Amazon SNS o i bucket Amazon S3 e l'operazione `getObject` è stata eliminata . Per ulteriori informazioni, vedere Concessione di autorizzazioni personalizzate per gli CloudTrail utenti.	29 settembre 2020
Documentazione aggiornata	Questo aggiornamento supporta la seguente versione di patch per la CloudTrail Processing Library: Aggiorna i riferimenti ai file.jar nella guida per l'utente per utilizzar e la versione più recente, -1.3.0.jar. aws-cloudtrail-processing-library Per ulteriori informazioni, vedere Using the CloudTrail Processing Library e Processing Library on. CloudTrail GitHub	28 agosto 2020
Aggiunta del supporto di un servizio	Questa release supporta AWS Outposts. Consulta Servizi e integrazioni AWS CloudTrail supportati.	28 agosto 2020

Funzionalità aggiunta	AWS CloudTrail Insights introduce i campi di attribuzione per gli eventi CloudTrail Insights. I campi di attribuzione mostrano le identità degli utenti principali, gli agenti dell'utente e i codici di errore associati all'attività anomala che attiva gli eventi Insights. Per il confronto, i campi di attribuzione mostrano anche le identità degli utenti principali, gli agenti dell'utente e i codici di errore associati ad attività normali o di riferimento. Per ulteriori informazioni, consulta Logging Insights events.	13 agosto 2020
Funzionalità aggiunta	La AWS CloudTrail console ha un nuovo look progettato per renderla più facile da usare. La Guida per AWS CloudTrail l'utente è stata aggiornata con modifiche alle procedure relative all'esecuzione di attività nella console, come la creazione di percorsi, l'aggiornamento dei percorsi e il download della cronologia degli eventi.	13 agosto 2020
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Interactive Video Service Consulta Servizi e integrazioni AWS CloudTrail supportati.	15 luglio 2020

Aggiunta del supporto di un servizio	Questa versione supporta Amazon Honeycode. Consulta Servizi e integrazioni AWS CloudTrail supportati.	24 giugno 2020
Aggiunta del supporto di un servizio	Questa release supporta Amazon Macie. Consulta Servizi e integrazioni AWS CloudTrail supportati.	19 maggio 2020
Aggiunta del supporto di un servizio	Questa release supporta Amazon Kendra. Consulta Servizi e integrazioni AWS CloudTrail supportati.	13 maggio 2020
Aggiunta del supporto di un servizio	Questa release supporta AWS IoT SiteWise. Consulta Servizi e integrazioni AWS CloudTrail supportati.	29 aprile 2020
Aggiunto il supporto per una Regione	Questa versione supporta una regione aggiuntiva: Europa (Milano). Consulta Regioni supportate in AWS CloudTrail.	28 aprile 2020
Aggiunta di assistenza e supporto per una Regione	Questa versione supporta Amazon AppFlow. Consulta Servizi e integrazioni AWS CloudTrail supportati. È stato aggiunto anche il Support per la regione Africa (Città del Capo). Consulta Regioni supportate in AWS CloudTrail.	22 aprile 2020

Funzionalità aggiunta	AWS KMS Le azioni ad alto volume come `EncryptDecrypt`, e `GenerateDataKey` vengono ora registrate come eventi di lettura. Se scegli di registrar e tutti AWS KMS gli eventi sul tuo percorso e scegli anche di registrare gli eventi di gestione di Write, il percorso registra AWS KMS le azioni pertinent i come`Disable`, e. `Delete ScheduleKey`	7 aprile 2020
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CodeGuru Reviewer. Consulta Servizi e integrazioni AWS CloudTrail supportati.	7 febbraio 2020
Aggiunta del supporto di un servizio	Questa versione supporta il servizio Amazon Managed Apache Cassandra. Consulta Servizi e integrazioni AWS CloudTrail supportati.	17 gennaio 2020
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Connect. Consulta Servizi e integrazioni AWS CloudTrail supportati.	13 dicembre 2019

Documentazione aggiornata	Questo aggiornamento supporta la seguente versione di patch per la CloudTrail Processing Library: Aggiorna i riferimenti ai file.jar nella guida per l'utente per utilizzar e la versione più recente, aws-cloudtrail-processing-l ibrary -1.2.0.jar. Per ulteriori informazioni, vedere Using the CloudTrail Processing Library e Processing Library on. CloudTrail GitHub	21 novembre 2019
Funzionalità aggiunta	Questa versione supporta AWS CloudTrail Insights per aiutarti a rilevare attività insolite nel tuo account. Consulta Registrazione di eventi Insights per i percorsi.	20 novembre 2019
Funzionalità aggiunta	Questa versione aggiunge un'opzione per filtrare AWS Key Management Service gli eventi da una traccia. Consulta Creazione di un trail.	20 novembre 2019
Aggiunta del supporto di un servizio	Questa versione supporta AWS CodeStar le notifiche. Consulta Servizi e integrazioni AWS CloudTrail supportati.	7 novembre 2019

Funzionalità aggiunta	Questa versione supporta l'aggiunta di tag quando si crea un trail in CloudTrail, indipendentemente dal fatto che si utilizzi la CloudTrai l console o l'API. Questa versione aggiunge due nuovi APIs, `GetTrail` e `ListTrail s` .	1° novembre 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS App Mesh. Consulta Servizi e integrazioni AWS CloudTrail supportati.	17 ottobre 2019
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Translate. Consulta Servizi e integrazioni AWS CloudTrail supportati.	17 ottobre 2019
Aggiornamento della documentazione	L'argomento Servizi non supportati è stato ripristinato e aggiornato per includere solo i AWS servizi che attualmen te non registrano gli eventi. CloudTrail Consulta Servizi non supportati di CloudTrail .	7 ottobre 2019

Aggiornamento della documentazione	La documentazione è stata aggiornata con le modifiche alla policy `AWSCloudTrailFullAccess`. Un esempio di policy che mostra le autorizzazioni equivalenti a `AWSCloudTrailFullAccess` è stato aggiornato per limitare le risorse su cui l'operazione `iam:PassRole` può intervenire a quelle che corrispondono alla seguente istruzione di condizione: `"iam:PassedToService": "cloudtrail.amazonaws.com"`. Consulta Esempi di policy basate su identità di AWS CloudTrail.	24 settembre 2019
Aggiornamento della documentazione	La documentazione è stata aggiornata con un nuovo argomento, Gestione CloudTrail dei costi, per aiutarvi a ottenere i dati di registro necessari CloudTrail rispettando il budget.	3 settembre 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS Control Tower. Consulta Servizi e integrazioni AWS CloudTrail supportati.	13 agosto 2019

Aggiunto il supporto per una Regione	Questa versione supporta una Regione aggiuntiva: Medio Oriente (Bahrein). Consulta Regioni supportate in AWS CloudTrail.	29 luglio 2019
Aggiornamento della documentazione	La documentazione è stata aggiornata con informazioni sulla sicurezza per CloudTrai l. Consulta Sicurezza in AWS CloudTrail.	3 luglio 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS Ground Station. Consulta Servizi e integrazioni AWS CloudTrail supportati.	6 giugno 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS IoT Things Graph. Consulta Servizi e integrazioni AWS CloudTrail supportati.	4 giugno 2019
Aggiunta del supporto di un servizio	Questa release supporta Amazon AppStream 2.0. Consulta Servizi e integrazioni AWS CloudTrail supportati.	25 aprile 2019
Aggiunto il supporto per una Regione	Questa versione supporta una Regione aggiuntiva: Asia Pacifico (Hong Kong). Consulta Regioni supportate in AWS CloudTrail.	24 aprile 2019
Aggiunta del supporto di un servizio	Questa versione supporta il servizio gestito da Amazon per Apache Flink. Consulta Servizi e integrazioni AWS CloudTrail supportati.	22 marzo 2019

Aggiunta del supporto di un servizio	Questa release supporta AWS Backup. Consulta Servizi e integrazioni AWS CloudTrail supportati.	4 febbraio 2019
Aggiunta del supporto di un servizio	Questa versione supporta Amazon WorkLink. Consulta Servizi e integrazioni AWS CloudTrail supportati.	23 gennaio 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS Cloud9. Consulta Servizi e integrazioni AWS CloudTrail supportati.	21 gennaio 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS Elemental MediaLive. Consulta Servizi e integrazioni AWS CloudTrail supportati.	19 gennaio 2019
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Comprehend. Consulta Servizi e integrazioni AWS CloudTrail supportati.	18 gennaio 2019
Aggiunta del supporto di un servizio	Questa release supporta AWS Elemental MediaPackage. Consulta Servizi e integrazioni AWS CloudTrail supportati.	21 dicembre 2018
Aggiunto il supporto per una Regione	Questa release supporta una Regione aggiuntiva: UE (Stoccolma). Consulta Regioni supportate in AWS CloudTrail.	11 dicembre 2018

Aggiornamento della documentazione	La documentazione è stata aggiornata con informazioni sui servizi supportati e non supportati. Consulta Servizi e integrazioni AWS CloudTrail supportati.	3 dicembre 2018
Aggiunta del supporto di un servizio	Questa versione supporta AWS Resource Access Manager (AWS RAM). Consulta Servizi e integrazioni AWS CloudTrail supportati.	20 novembre 2018
Funzionalità aggiornate	Questa versione supporta la creazione di un trail in CloudTrail cui vengono registrati gli eventi di tutti AWS gli account di un'organi zzazione. AWS Organizations Consulta Creazione di un trail per un'organizzazione.	19 novembre 2018
Aggiunta del supporto di un servizio	Questa versione supporta l'API SMS and Voice di Amazon Pinpoint. Consulta Servizi e integrazioni AWS CloudTrail supportati.	16 novembre 2018
Aggiunta del supporto di un servizio	Questa release supporta AWS IoT Greengrass. Consulta Servizi e integrazioni AWS CloudTrail supportati.	29 ottobre 2018

Documentazione aggiornata	Questo aggiornamento supporta la seguente versione di patch per la CloudTrail Processing Library: Aggiorna i riferimenti ai file.jar nella guida per l'utente per utilizzar e la versione più recente, aws-cloudtrail-processing-l ibrary -1.1.3.jar. Per ulteriori informazioni, vedere Using the CloudTrail Processing Library e Processing Library on. CloudTrail GitHub	18 ottobre 2018
Funzionalità aggiunta	Questa release supporta l'utilizzo di filtri aggiuntivi nella cronologia di eventi. Vedi Visualizzazione CloudTrail degli eventi nella CloudTrail console.	18 ottobre 2018
Funzionalità aggiunta	Questa versione supporta l'uso di Amazon Virtual Private Cloud (Amazon VPC) per stabilire una connessione privata tra il VPC e AWS CloudTrail. Vedi Utilizzo AWS CloudTrail con gli endpoint VPC dell'interfaccia.	9 agosto 2018
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Data Lifecycle Manager. Consulta Servizi e integrazioni AWS CloudTrail supportati.	24 luglio 2018

Aggiunta del supporto di un servizio	Questa versione supporta Amazon MQ. Consulta Servizi e integrazioni AWS CloudTrail supportati.	19 luglio 2018
Aggiunta del supporto di un servizio	Questa versione supporta AWS Mobile CLI. Consulta Servizi e integrazioni AWS CloudTrail supportati.	29 giugno 2018
AWS CloudTrail notifica della cronologia della documentazione disponibile tramite feed RSS	Ora puoi ricevere notifiche sugli aggiornamenti della AWS CloudTrail documentazione iscrivendoti a un feed RSS.	29 giugno 2018

Aggiornamenti precedenti

La tabella seguente descrive la cronologia dei rilasci della documentazione AWS CloudTrail precedenti al 29 giugno 2018.

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta Amazon RDS Performance Insights. Per ulteriori informazioni, consulta Servizi e integrazioni CloudTrail supportati.	21 giugno 2018
Funzionalità aggiunta	Questa versione supporta la registrazione di tutti gli eventi CloudTrail di gestione nella cronologia degli eventi. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.	14 giugno 2018
Aggiunta del supporto di un servizio	Questa release supporta Gestione dei costi e fatturazione AWS. Consultare CloudTrail servizi e integrazioni supportati.	7 giugno 2018

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consultare CloudTrail servizi e integrazioni supportati.	5 giugno 2018
Documentazione aggiornata	Questo aggiornamento supporta la seguente release patch della libreria di elaborazione CloudTrail: • Aggiornate i riferimenti ai file.jar nella guida per l'utente per utilizzare la versione più recente, aws-cloudtrail-processing-library -1.1.2.jar. Per ulteriori informazioni, vedere Utilizzo della libreria CloudTrail di elaborazione e Processing Library on. CloudTrail GitHub	16 maggio 2018
Aggiunta del supporto di un servizio	Questa release supporta Gestione dei costi e fatturazione AWS. Consultare CloudTrail servizi e integrazioni supportati.	7 giugno 2018
Aggiunta del supporto di un servizio	Questa release supporta Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consultare CloudTrail servizi e integrazioni supportati.	5 giugno 2018
Documentazione aggiornata	Questo aggiornamento supporta la seguente release patch della libreria di elaborazione CloudTrail: • Aggiorna i riferimenti ai file.jar nella guida per l'utente per utilizzare la versione più recente, aws-cloudtrail-processing-library -1.1.2.jar. Per ulteriori informazioni, vedere Utilizzo della libreria CloudTrail di elaborazione e Processing Library on. CloudTrail GitHub	16 maggio 2018

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta AWS X-Ray. Consultare CloudTrail servizi e integrazioni supportati.	25 aprile 2018
Aggiunta del supporto di un servizio	Questa versione supporta AWS IoT Analytics. Consultare CloudTrail servizi e integrazioni supportati.	23 aprile 2018
Aggiunta del supporto di un servizio	Questa versione supporta Secrets Manager. Consultar e CloudTrail servizi e integrazioni supportati.	10 aprile 2018
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Rekognition. Consultare CloudTrail servizi e integrazioni supportati.	6 aprile 2018
Aggiunta del supporto di un servizio	Questa versione supporta AWS Private Certifica te Authority (PCA). Consultare CloudTrail servizi e integrazioni supportati.	4 aprile 2018
Funzionalità aggiunta	Questa versione supporta la semplificazione della ricerca nei file di CloudTrail registro con Amazon Athena. Puoi creare automaticamente tabelle per interrogare i log direttamente dalla CloudTrail console e utilizzarle per eseguire query in Athena. Per ulteriori informazioni, consulta Creazione CloudTrail servizi e integrazioni supportati di una tabella per i CloudTrail log nella console. CloudTrail	15 marzo 2018
Aggiunta del supporto di un servizio	Questa release supporta AWS AppSync. Consultare CloudTrail servizi e integrazioni supportati.	13 febbraio 2018
È stato aggiunto il supporto per una regione	Questa versione supporta una Regione aggiuntiv a: Asia Pacifico (Osaka-Locale) (ap-northeast-3). Consultare CloudTrail Regioni supportate.	12 febbraio 2018
Aggiunta del supporto di un servizio	Questa release supporta AWS Shield. Consultare CloudTrail servizi e integrazioni supportati.	12 febbraio 2018

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta Amazon SageMaker AI. Consultare CloudTrail servizi e integrazioni supportati.	11 gennaio 2018
Aggiunta del supporto di un servizio	Questa release supporta AWS Batch. Consultare CloudTrail servizi e integrazioni supportati.	10 gennaio 2018
Funzionalità aggiunta	Questa versione supporta l'estensione della quantità di attività dell'account disponibile nella cronologia CloudTrail degli eventi a 90 giorni. Puoi anche personalizzare la visualizzazione delle colonne per migliorare la visualizzazione dei tuoi CloudTrail eventi. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.	12 dicembre 2017
Aggiunta del supporto di un servizio	Questa versione supporta Amazon WorkMail. Consultare CloudTrail servizi e integrazioni supportati.	12 dicembre 2017
Aggiunta del supporto di un servizio	Questa versione supporta Alexa for Business AWS Elemental MediaConvert e. AWS Elemental MediaStore Consultare CloudTrail servizi e integrazioni supportati.	1° dicembre 2017
Ulteriori funzionalità e documentazione	Questa versione supporta la registrazione degli eventi relativi ai dati per le AWS Lambda funzioni. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	30 novembre 2017
Ulteriori funzionalità e documentazione	Questa versione supporta la registrazione degli eventi relativi ai dati per le AWS Lambda funzioni. Per ulteriori informazioni, consulta Registrazione degli eventi di dati.	30 novembre 2017

Modifica	Descrizione	Data di rilascio
Ulteriori funzionalità e documentazione	Questa versione supporta i seguenti aggiornamenti alla CloudTrail Processing Library: • Aggiunta del supporto per l'identificazione booleana di eventi di gestione. • Aggiorna la versione CloudTrail dell'evento alla 1.06. Per ulteriori informazioni, vedere Utilizzo della libreria CloudTrail di elaborazione e CloudTrail Processing Library on GitHub.	30 novembre 2017
Aggiunta del supporto di un servizio	Questa release supporta AWS Glue. Consultare CloudTrail servizi e integrazioni supportati.	7 novembre 2017
Nuova documentazione	In questa versione è stato aggiunto il nuovo argomento Quote in AWS CloudTrail.	19 ottobre 2017
Documentazione aggiornata	Questa versione aggiorna la documentazione APIs supportata nella cronologia degli CloudTrail eventi per Amazon Athena, AWS CodeBuild Amazon Elastic Container Registry e. AWS Migration Hub	13 ottobre 2017
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Chime. Consultare CloudTrail servizi e integrazioni supportati.	27 settembre 2017
Ulteriori funzionalità e documentazione	Questa versione supporta la configurazione della registrazione degli eventi dei dati per tutti i bucket Amazon S3 presenti nel tuo account. AWS Consultare Registrazione degli eventi di dati.	20 settembre 2017
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Lex. Consultare CloudTrail servizi e integrazioni supportati.	15 agosto 2017

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta AWS Migration Hub. Consultare CloudTrail servizi e integrazioni supportati.	14 agosto 2017
Ulteriori funzionalità e documentazione	Questa versione supporta CloudTrail l'attivazione per impostazione predefinita per tutti gli AWS account. Nella cronologia di eventi CloudTrail sono disponibili gli ultimi sette giorni dell'attività dell'account, mentre gli eventi più recenti vengono visualizzati nel pannello di controllo della console. La caratteristica precedent emente nota come cronologia delle attività delle API è stata sostituita dalla cronologia degli eventi.	14 agosto 2017
Ulteriori funzionalità e documentazione	Questa versione supporta il download di eventi dalla CloudTrail console nella pagina della cronologia delle attività dell'API. È possibile scaricare gli eventi in formato JSON o CSV. Per ulteriori informazioni, consulta Download di eventi.	27 luglio 2017
Funzionalità aggiunta	Questa versione supporta la registrazione delle operazioni delle API a livello di oggetti Amazon S3 in due regioni aggiuntive: Europa (Londra) e Canada (Centrale). Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro.	19 luglio 2017
Aggiunta del supporto di un servizio	Questa versione supporta la APIs ricerca di Amazon CloudWatch Events nella funzionalità di cronologia delle attività dell' CloudTrail API.	27 giugno 2017

Modifica	Descrizione	Data di rilascio
Ulteriori funzionalità e documentazione	Questa versione supporta funzionalità aggiuntive APIs nella cronologia delle attività delle CloudTrail API per i seguenti servizi: • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	27 giugno 2017
Aggiunta del supporto di un servizio	Questa release supporta AWS CodeStar. Consultare CloudTrail servizi e integrazioni supportati.	14 giugno 2017

Modifica	Descrizione	Data di rilascio

Ulteriori funzionalità e documentazione	Questa versione supporta i seguenti aggiornamenti alla CloudTrail Processing Library:
	• Aggiunge il supporto per diversi formati per i messaggi SQS dalla stessa coda SQS per identific are CloudTrail i file di registro. Sono supportati i formati seguenti:
	  • Notifiche CloudTrail inviate a un argomento SNS
	  • Notifiche inviate da Amazon S3 a un argomento SNS
	  • Notifiche inviate direttamente da Amazon S3 a una coda SQS
	• Aggiunta del supporto per la proprietà `deleteMes sageUponFailure` , che è possibile utilizzare per eliminare i messaggi che non possono essere elaborati.
	
	Per ulteriori informazioni, vedere Utilizzo della libreria CloudTrail di elaborazione e CloudTrail Processing Library on GitHub.
		1 giugno 2017

Aggiunta del supporto di un servizio	Questa versione supporta Amazon Athena. Consultare CloudTrail servizi e integrazioni supportati.	19 maggio 2017
Funzionalità aggiunta	Questa versione supporta l'invio di eventi di dati ad Amazon CloudWatch Logs. Per ulteriori informazioni sulla configurazione del trail per registrare gli eventi di dati, consultare Eventi di dati. Per ulteriori informazioni sull'invio di eventi a CloudWatch Logs, consulta. Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs	9 maggio 2017

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta il servizio di Marketplace AWS misurazione. Consultare CloudTrail servizi e integrazioni supportati.	2 maggio 2017
Aggiunta del supporto di un servizio	Questa versione supporta Amazon QuickSight. Consultare CloudTrail servizi e integrazioni supportati.	28 aprile 2017
Ulteriori funzionalità e documentazione	Questa release supporta un'esperienza di console aggiornata per la creazione di nuovi trail. Ora è possibile configurare un nuovo trail per registrare gli eventi di gestione e dati. Per ulteriori informazioni, consulta Creazione di un percorso con la CloudTrail console.	11 aprile 2017
Aggiunta di documenta zione	Se CloudTrail non invia i log al tuo bucket S3 o non invia notifiche SNS da alcune regioni del tuo account, potrebbe essere necessario aggiornare le politiche. Per ulteriori informazioni su come aggiornare la policy del bucket S3, consultare Errori di configurazione comuni della policy Amazon S3. Per ulteriori informazioni su come aggiornare la policy dell'argomento SNS, consultare CloudTrail non sta inviando notifiche per una regione.	31 marzo 2017
Aggiunta del supporto di un servizio	Questa release supporta AWS Organizations. Consultare CloudTrail servizi e integrazioni supportati.	27 febbraio 2017
Ulteriori funzionalità e documentazione	Questa release supporta un'esperienza di console aggiornata per la configurazione dei trail per la registrazione degli eventi di gestione e dati. Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro.	10 febbraio 2017

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta Amazon Cloud Directory. Consultare CloudTrail servizi e integrazioni supportati.	26 gennaio 2017
Ulteriori funzionalità e documentazione	Questa versione supporta APIs la ricerca AWS CodeCommit di Amazon GameLift Servers e AWS Managed Services nella cronologia delle attività delle CloudTrail API.	26 gennaio 2017
Funzionalità aggiunta	Questa release supporta l'integrazione con AWS Health Dashboard. Puoi utilizzarlo AWS Health Dashboard per identific are se i tuoi percorsi non sono in grado di inviare log a un argomento SNS o a un bucket S3. Ciò può verificar si in caso di problemi con la policy per il bucket S3 o l'argomento SNS. AWS Health Dashboard ti informa sui percorsi interessati e consiglia modi per correggere la politica. Per ulteriori informazioni, consulta la AWS Health Guida per l'utente di .	24 gennaio 2017
Ulteriori funzionalità e documentazione	Questa release supporta i filtri in base all'origine degli eventi nella console CloudTrail. La fonte dell'even to mostra il AWS servizio a cui è stata effettuata la richiesta. Per ulteriori informazioni, consulta Visualizzazione degli eventi di gestione recenti con la console.	12 gennaio 2017
Aggiunta del supporto di un servizio	Questa release supporta AWS CodeCommit. Consultare CloudTrail servizi e integrazioni supportati.	11 gennaio 2017
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Lightsail. Consultar e CloudTrail servizi e integrazioni supportati.	23 dicembre 2016

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta AWS Managed Services. Consultare CloudTrail servizi e integrazioni supportati.	21 dicembre 2016
È stato aggiunto il supporto per una regione	Questa versione supporta la regione Europa (Londra). Consultare CloudTrail Regioni supportate.	13 dicembre 2016
È stato aggiunto il supporto per una regione	Questa versione supporta la regione Canada (Centrale). Consultare CloudTrail Regioni supportate.	8 dicembre 2016
Aggiunta del supporto di un servizio	Questa versione supporta AWS CodeBuild SeeCloudTrail servizi e integrazioni supportati. Questa release supporta AWS Health. Consultare CloudTrail servizi e integrazioni supportati. Questa release supporta AWS Step Functions. Consultare CloudTrail servizi e integrazioni supportati.	1° dicembre 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Polly. Consultare CloudTrail servizi e integrazioni supportati.	30 novembre 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS OpsWorks for Chef Automate. Consultare CloudTrail servizi e integrazioni supportati.	23 novembre 2016

Modifica	Descrizione	Data di rilascio
Ulteriori funzionalità e documentazione	Questa release supporta la configurazione del trail in modo che registri gli eventi di sola lettura, gli eventi di sola scrittura o tutti gli eventi. CloudTrail supporta la registrazione di operazioni API a livello di oggetto di Amazon S3 `GetObject` come`PutObject` , e. `DeleteObject` È possibile configurare i trail in modo che registrino le operazioni delle API a livello di oggetti. Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro.	21 novembre 2016
Ulteriori funzionalità e documentazione	Questa release supporta valori aggiuntivi per il campo `type` nell'elemento `userIdentity` : `AWSAccount` e `AWSService` . Per ulteriori informazioni, consultare la Campi per `userIdentity` .	16 novembre 2016
Aggiunta del supporto di un servizio	Questa versione supporta Application Auto Scaling. Consultare CloudTrail servizi e integrazioni supportati.	31 ottobre 2016
È stato aggiunto il supporto per una regione	Questa versione supporta la regione Stati Uniti orientali (Ohio). Consultare CloudTrail Regioni supportate.	17 ottobre 2016
Ulteriori funzionalità e documentazione	Questa versione supporta la registrazione di eventi di servizio non AWS API. Per ulteriori informazioni, consulta Servizio AWS eventi.	23 settembre 2016
Ulteriori funzionalità e documentazione	Questa versione supporta l'utilizzo della CloudTrai l console per visualizzare i tipi di risorse supportati da. AWS Config Per ulteriori informazioni, consulta Visualizzazione di risorse a cui viene fatto riferimento tramite AWS Config.	7 luglio 2016

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta AWS Service Catalog. Consultare CloudTrail servizi e integrazioni supportati.	6 luglio 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Elastic File System (Amazon EFS). Consultare CloudTrail servizi e integrazioni supportati.	28 giugno 2016
È stato aggiunto il supporto per una regione	Questa versione supporta una regione aggiuntiva: Asia Pacifico (Mumbai) (ap-south-1). Consultare CloudTrail Regioni supportate.	27 giugno 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS Application Discovery Service. Consultare CloudTrail servizi e integrazioni supportati.	12 maggio 2016
Aggiunta del supporto di un servizio	Questa versione supporta CloudWatch i registri nella regione Sud America (San Paolo). Per ulteriori informazioni, consulta Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs.	6 maggio 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS WAF. Consultare CloudTrail servizi e integrazioni supportati.	28 aprile 2016
Aggiunta del supporto di un servizio	Questa release supporta Supporto AWS. Consultare CloudTrail servizi e integrazioni supportati.	21 aprile 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Inspector. Consultare CloudTrail servizi e integrazioni supportati.	20 aprile 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS IoT. Consultare CloudTrail servizi e integrazioni supportati.	11 aprile 2016

Modifica	Descrizione	Data di rilascio
Ulteriori funzionalità e documentazione	Questa versione supporta le chiamate API logging AWS Security Token Service (AWS STS) effettuate con Security Assertion Markup Language (SAML) e la federazione delle identità web. Per ulteriori informazioni, consulta Valori per AWS STS APIs con SAML e la federazione delle identità web.	28 marzo 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS Certificate Manager. Consultare CloudTrail servizi e integrazioni supportati.	25 marzo 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Data Firehose. Consultare CloudTrail servizi e integrazioni supportati.	17 marzo 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CloudWatch Logs. Consultare CloudTrail servizi e integrazioni supportati.	10 marzo 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Cognito. Consultare CloudTrail servizi e integrazioni supportati.	18 febbraio 2016
Aggiunta del supporto di un servizio	Questa release supporta AWS Database Migration Service. Consultare CloudTrail servizi e integrazioni supportati.	4 febbraio 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon GameLift Servers (Amazon GameLift Servers). Consultare CloudTrail servizi e integrazioni supportati.	27 gennaio 2016
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CloudWatch Events. Consultare CloudTrail servizi e integrazioni supportati.	16 gennaio 2016
È stato aggiunto il supporto per una regione	Questa versione supporta una Regione aggiuntiva: Asia Pacifico (Seoul) (ap-northeast-2). Consultare CloudTrail Regioni supportate.	6 gennaio 2016

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Elastic Container Registry (Amazon ECR). Consultare CloudTrail servizi e integrazioni supportati.	21 dicembre 2015
Ulteriori funzionalità e documentazione	Questa versione supporta l'attivazione CloudTrail in tutte le regioni e il supporto per più percorsi per regione. Per ulteriori informazioni, consulta Lavorare con i CloudTrail sentieri.	17 dicembre 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Machine Learning. Consultare CloudTrail servizi e integrazioni supportati.	10 dicembre 2015
Ulteriori funzionalità e documentazione	Questa release supporta la crittografia dei file di log, la convalida dell'integrità dei file di log e il tagging. Per ulteriori informazioni, consultare Crittografia di file di CloudTrail registro, file digest e archivi dati di eventi con AWS KMS chiavi (SSE-KMS), Convalida dell'integrità dei file di CloudTrail registro e Aggiornamento di un percorso con la CloudTrail console.	1° ottobre 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon OpenSearch Service. Consultare CloudTrail servizi e integrazioni supportati.	1° ottobre 2015
Aggiunta del supporto di un servizio	Questa versione supporta gli eventi a livello di bucket Amazon S3. Consultare CloudTrail servizi e integrazioni supportati.	1 settembre 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS Device Farm. Consultare CloudTrail servizi e integrazioni supportati.	13 luglio 2015
Aggiunta del supporto di un servizio	Questa versione supporta Gateway Amazon API. Consultare CloudTrail servizi e integrazioni supportati.	9 luglio 2015

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta CodePipeline. Consultare CloudTrail servizi e integrazioni supportati.	9 luglio 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon DynamoDB. Consultare CloudTrail servizi e integrazioni supportati.	28 maggio 2015
Aggiunta del supporto di un servizio	Questa versione supporta CloudWatch i log nella regione Stati Uniti occidentali (California settentri onale). Per ulteriori informazioni sul CloudTrail supporto per il monitoraggio CloudWatch dei registri, vedere. Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs	19 maggio 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS Directory Service. Consultare CloudTrail servizi e integrazioni supportati.	14 maggio 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Simple Email Service (Amazon SES). Consultare CloudTrail servizi e integrazioni supportati.	7 maggio 2015
Aggiunta del supporto di un servizio	Questa versione supporta il servizio Amazon Elastic Container. Consulta CloudTrail servizi e integrazioni supportati.	9 aprile 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS Lambda. Consultare CloudTrail servizi e integrazioni supportati.	9 aprile 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon WorkSpaces. Consultare CloudTrail servizi e integrazioni supportati.	9 aprile 2015

Modifica	Descrizione	Data di rilascio
	Questa versione supporta la ricerca delle AWS attività acquisite da CloudTrail (CloudTrail events). È possibile cercare e filtrare gli eventi correlati alla creazione , modifica o eliminazione nel proprio account. Per cercare questi eventi, puoi usare la CloudTrail console, AWS Command Line Interface (AWS CLI) o l' AWS SDK. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.	12 marzo 2015
Aggiunta del supporto di servizi e di nuova documentazione	Questa versione supporta Amazon CloudWatch Logs nelle regioni Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Tokyo) ed Europa (Francofo rte). Per ulteriori informazioni, consulta Invio di eventi ai CloudWatch registri.	5 marzo 2015
Nuova documentazione	Una nuova sezione che descrive CloudTrail il supporto per gli endpoint regionali AWS Security Token Service (AWS STS) è stata aggiunta alla pagina CloudTrail Concetti.	17 febbraio 2015
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Route 53. Consultare CloudTrail servizi e integrazioni supportati.	11 febbraio 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS Config. Consultare CloudTrail servizi e integrazioni supportati.	10 febbraio 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS CloudHSM. Consultare CloudTrail servizi e integrazioni supportati.	8 gennaio 2015
Aggiunta del supporto di un servizio	Questa release supporta AWS CodeDeploy. Consultar e CloudTrail servizi e integrazioni supportati.	17 dicembre 2014

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa release supporta AWS Storage Gateway. Consultare CloudTrail servizi e integrazioni supportati.	16 dicembre 2014
È stato aggiunto il supporto per una regione	Questa versione supporta una regione aggiuntiva: us-gov-west -1 (AWS GovCloud (US-West)). Consultare CloudTrail Regioni supportate.	16 dicembre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon S3 Glacier. Consultare CloudTrail servizi e integrazioni supportati.	11 dicembre 2014
Aggiunta del supporto di un servizio	Questa release supporta AWS Data Pipeline. Consultare CloudTrail servizi e integrazioni supportati.	2 dicembre 2014
Aggiunta del supporto di un servizio	Questa release supporta AWS Key Management Service. Consultare CloudTrail servizi e integrazioni supportati.	12 novembre 2014
Nuova documentazione	Alla guida è stata aggiunta una nuova sezione: Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs. Descrive come utilizzare Amazon CloudWatch Logs per monitorare gli eventi di CloudTrail registro.	10 novembre 2014
Nuova documentazione	Alla guida è stata aggiunta una nuova sezione: Utilizzo della libreria CloudTrail di elaborazione. Fornisce informazioni su come scrivere un processore di CloudTrail log in Java utilizzando la AWS CloudTrail Processing Library.	5 novembre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Elastic Transcoder. Consultare CloudTrail servizi e integrazioni supportati.	27 ottobre 2014

Modifica	Descrizione	Data di rilascio
È stato aggiunto il supporto per una regione	Questa versione supporta una regione aggiuntiva: eu-central-1 (Europa (Francoforte)). Consultare CloudTrail Regioni supportate.	23 ottobre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CloudSearch. Consultare CloudTrail servizi e integrazioni supportati.	16 ottobre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Simple Notification Service. Consultare CloudTrail servizi e integrazioni supportati.	09 ottobre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon ElastiCache. Consultare CloudTrail servizi e integrazioni supportati.	15 settembre 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon WorkDocs. Consultare CloudTrail servizi e integrazioni supportati.	27 agosto 2014
Aggiunti nuovi contenuti	Questa versione include un argomento che illustra la registrazione degli eventi di accesso. Consultare AWS Management Console eventi di accesso.	24 luglio 2014
Aggiunti nuovi contenuti	L'elemento eventVersion in questa versione è stato aggiornato alla versione 1.02 e sono stati aggiunti tre nuovi campi. Consultare CloudTrail registrare contenuti per eventi di gestione, dati e attività di rete.	18 luglio 2014
Aggiunta del supporto di un servizio	Questa versione supporta Auto Scaling (consultare CloudTrail servizi e integrazioni supportati).	17 luglio 2014
È stato aggiunto il supporto per una regione	Questa versione supporta tre Regioni aggiuntive: (Asia Pacifico (Singapore) (ap-southeast-1), (Asia Pacifico (Tokyo) (ap-northeast-1), (Sud America (San Paolo) (sa-east-1). Consultare CloudTrail Regioni supportate.	30 giugno 2014

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Redshift. Consultare CloudTrail servizi e integrazioni supportati.	10 giugno 2014
Aggiunta del supporto di un servizio	Questa release supporta OpsWorks. Consultare CloudTrail servizi e integrazioni supportati.	5 giugno 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CloudFront. Consultare CloudTrail servizi e integrazioni supportati.	28 maggio 2014
È stato aggiunto il supporto per una regione	Questa versione supporta tre Regioni aggiuntive: Stati Uniti occidentali (California settentrionale) (us-west-1), Europa (Irlanda) (eu-west-1), Asia Pacifico (Sydney) (ap-southeast-2). Consultare CloudTrail Regioni supportate.	13 maggio 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Simple Workflow Service. Consultare CloudTrail servizi e integrazioni supportati.	9 maggio 2014
Aggiunti nuovi contenuti	Questa versione include argomenti che illustrano la condivisione di file di log tra account. Consultare Condivisione di file di CloudTrail registro tra AWS account.	2 maggio 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon CloudWatch. Consultare CloudTrail servizi e integrazioni supportati.	28 aprile 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon Kinesis. Consultare CloudTrail servizi e integrazioni supportati.	22 aprile 2014
Aggiunta del supporto di un servizio	Questa release supporta AWS Direct Connect. Consultare CloudTrail servizi e integrazioni supportati.	11 aprile 2014
Aggiunta del supporto di un servizio	Questa versione supporta Amazon EMR. Consultare CloudTrail servizi e integrazioni supportati.	4 aprile 2014

Modifica	Descrizione	Data di rilascio
Aggiunta del supporto di un servizio	Questa versione supporta Elastic Beanstalk. Consultare CloudTrail servizi e integrazioni supportati.	2 aprile 2014
Aggiunta del supporto di un servizio	Questa release supporta AWS CloudFormation. Consultare CloudTrail servizi e integrazioni supportati.	7 marzo 2014
Nuova guida	Questa versione introduce AWS CloudTrail.	13 novembre 2013

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.